

MobileNext Broadband Gateway

Redundancy



Published: 2012-04-11

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

Copyright © 2012, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

MobileNext Broadband Gateway Redundancy

Copyright © 2012, Juniper Networks, Inc.

All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	ix
	Documentation and Release Notes	ix
	Supported Platforms	ix
	Documentation Conventions	ix
	Documentation Feedback	xi
	Requesting Technical Support	xi
	Self-Help Online Tools and Resources	xii
	Opening a Case with JTAC	xii
Part 1	Overview	
Chapter 1	Redundancy Overview	3
	Broadband Gateway Redundancy Overview	4
	Routing Engine Redundancy	4
	Session DPC Redundancy	5
	Interface Redundancy	6
	Understanding the Broadband Gateway Anchor Failover Behavior	7
Part 2	Configuration	
Chapter 2	Configuration Tasks	13
	Configuring Session DPC Redundancy	13
	Configuring Interface Redundancy	15
Chapter 3	Configuration Examples	17
	Example: Configuring Broadband Gateway Redundancy	17
Chapter 4	Configuration Statements	21
	[edit interfaces ams] Hierarchy Level	21
	[edit interfaces apfe] Hierarchy Level	22
	pfes	23
	service-pics	23
	session-pics	24
	apfe-group-set (Aggregated Packet Forwarding Engine)	25
	anchoring-options (Aggregated Packet Forwarding Engine)	26
	dedicated (IPsec)	27
	dial-options (IPsec)	27
	drop-member-traffic (Aggregated Multiservices)	28
	egress-key (Aggregated Multiservices)	29
	enable-rejoin (Aggregated Multiservices)	30
	family (Aggregated Multiservices)	31
	hash-keys (Aggregated Multiservices)	32

high-availability-options (Aggregated Multiservices)	34
ingress-key (Aggregated Multiservices)	35
interface (Packet Forwarding Engine)	36
interface (Services PIC)	38
interface (Session PIC)	39
interface-service (Aggregated Multiservices)	40
interfaces (Aggregated Multiservices)	41
interfaces (Aggregated Packet Forwarding Engine)	43
ipsec-interface-id (IPsec)	44
load-balancing-options (Aggregated Multiservices)	45
load-balancing-options (Aggregated Multiservices for Services Applications)	46
load-balancing-options (IPsec)	47
many-to-one (Aggregated Multiservices)	48
member-failure-options (Aggregated Multiservices)	49
member-interface (Aggregated Multiservices)	52
preferred-active (IPsec)	53
primary-list (Aggregated Packet Forwarding Engine)	54
redistribute-all-traffic (Aggregated Multiservices)	55
rejoin-timeout (Aggregated Multiservices)	56
resource-triggered (Aggregated Multiservices)	57
secondary (Aggregated Packet Forwarding Engine)	58
service-set (Aggregated Multiservices)	59
shared (IPsec)	61
system (MobileNext Broadband Gateway Interfaces)	61
unit (Aggregated Multiservices)	62
warm-standby (Aggregated Packet Forwarding Engine)	63

Part 3

Chapter 5

Administration

Operational Commands 67

request interface load-balancing revert (Aggregated Multiservices)	68
request interface load-balancing switchover (Aggregated Multiservices)	69
show services flows (Aggregated Multiservices)	70
show services nat mappings app	74
show services nat mappings eim	76
show services nat mappings summary	78
show services nat pool (Aggregated Multiservices)	79
show services nat statistics	82
show services service-sets summary	91
show services sessions (Aggregated Multiservices)	93
show interfaces anchor-group (Aggregated Packet Forwarding Engine)	100
show interfaces load-balancing (Aggregated Multiservices)	103
show services ipsec-vpn ipsec security-associations	106
show unified-edge ggsn-pgw system interfaces	110
show unified-edge sgw system interfaces	112

Part 4

Index

Index	117
-----------------	-----

List of Figures

Part 1	Overview	
Chapter 1	Redundancy Overview	3
	Figure 1: Redundancy Available on the Broadband Gateway	4
	Figure 2: Control Plane Anchor Operation Before Failure	7
	Figure 3: Control Plane Anchor Operation After Failure	8
	Figure 4: Pre- and Post-Failure PFE Datapaths	8
Part 2	Configuration	
Chapter 3	Configuration Examples	17
	Figure 5: Redundancy Example for the Broadband Gateway	18

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	x
	Table 2: Text and Syntax Conventions	x
Part 2	Configuration	
Chapter 4	Configuration Statements	21
	Table 3: Hash Keys Supported for AMS for Service Applications	33
	Table 4: Behavior of Member Interface After One Multiservices PIC Fails	49
	Table 5: Behavior of Member Interface After Two Multiservices PICs Fail	50
Part 3	Administration	
Chapter 5	Operational Commands	67
	Table 6: show services flows Output Fields	72
	Table 7: show services nat mappings app Output Fields	74
	Table 8: show services nat mappings eim Output Fields	76
	Table 9: show services nat mappings summary Output Fields	78
	Table 10: show services nat pool Output Fields	79
	Table 11: show services nat statistics Output Fields	82
	Table 12: show services service-sets summary Output Fields	91
	Table 13: show services sessions Output Fields	95
	Table 14: show interfaces anchor-group	100
	Table 15: show interfaces load-balancing Output Fields	103
	Table 16: show services ipsec-vpn ipsec security-associations Output Fields . .	106
	Table 17: show unified-edge ggsn-pgw system interfaces	110
	Table 18: show unified-edge sgw system interfaces Output Fields	112

About the Documentation

- Documentation and Release Notes on page ix
- Supported Platforms on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xi

Documentation and Release Notes

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

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

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

Supported Platforms

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

- MX240 Routers
- MX960 Routers
- MX480 Routers

Documentation Conventions

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

Table 1: Notice Icons


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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: <code>user@host> configure</code>
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: <code>[edit]</code> <code>root@# set system domain-name <i>domain-name</i></code>
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the <code>[edit protocols ospf area area-id]</code> hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	<code>stub <default-metric <i>metric</i>>;</code>

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

Convention	Description	Examples
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

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

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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

- [Redundancy Overview on page 3](#)

CHAPTER 1

Redundancy Overview

- [Broadband Gateway Redundancy Overview on page 4](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 7](#)

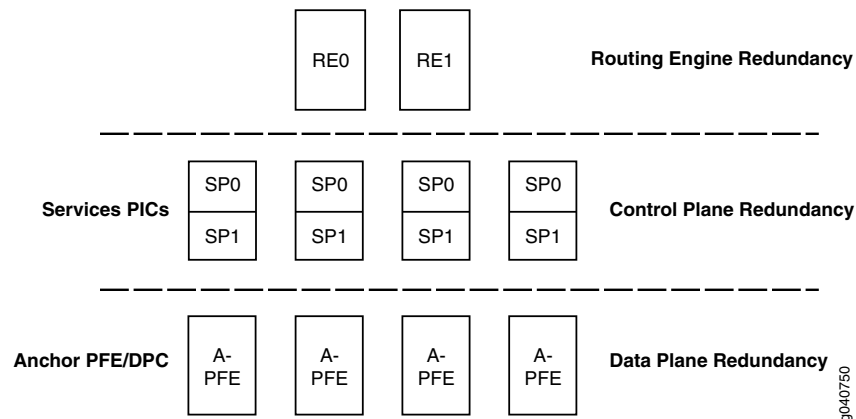
Broadband Gateway Redundancy Overview

The MobileNext Broadband Gateway chassis contains Routing Engines, session Dense Port Concentrators (DPCs), and interface DPCs or Modular Port Concentrators (MPCs) (housing PFEs). Whether used as a GPRS gateway support node (GGSN) or Packet Data Network Gateway (P-GW), service and interface cards running the mobility package are configured to provide redundancy similar to that between the Routing Engines. However, different types of redundancy are used for the different levels of hardware used in the broadband gateway.

The broadband gateway consists of Routing Engines (we recommend two), sessions DPCs (we recommend two or more), and interface PFEs (we recommend two or more DPCs or MPCs). Other service DPCs and interface cards can be installed, but only the elements configured to run the mobility software package can be part of the broadband gateway function. In other words, some elements of the broadband gateway might not be involved in mobile packet flows, but they implement a provider edge (PE) router function, related network address translation (NAT) or IPsec services, and so on. This topic describes only the mobile redundancy portion of the configuration.

Figure 1 on page 4 shows that redundancy is available for the Routing Engines, session DPCs, and interface PFEs (housed in interface DPCs or MPCs). However, there are important differences in each type.

Figure 1: Redundancy Available on the Broadband Gateway



This redundancy configuration overview covers:

- [Routing Engine Redundancy on page 4](#)
- [Session DPC Redundancy on page 5](#)
- [Interface Redundancy on page 6](#)

Routing Engine Redundancy

The Routing Engine is an Intel-based PCI platform that runs the Junos OS software on all product lines. The software processes that run on the Routing Engine oversee all of the functions that perform the mobility tasks running on the chassis. On the MobileNext

Broadband Gateway, there is 1:1 redundancy on the Routing Engines when two (the maximum) are installed.

When two Routing Engines are installed in the broadband gateway, both are powered on, but only one is active (the master). At boot time, both Routing Engines run an arbitration algorithm and elect one as master. The second Routing Engine is in standby mode and performs no functions. If the master Routing Engine fails, the standby unit takes over.

By default, the master Routing Engine is **RE0**. You can change the default master by including the appropriate **routing-engine** statement at the **[edit chassis redundancy]** hierarchy level.



NOTE: Although you can run the broadband gateway with only one Routing Engine, we do not recommend it.

The Routing Engine components are hot-pluggable. Removal or failure of the standby does not affect the function of the broadband gateway.

However, if the master Routing Engine is removed from the chassis:

- If there is only one Routing Engine, then packet forwarding halts until the Routing Engine is reinstalled and functioning normally.
- If there are two Routing Engines, packet forwarding halts while the standby Routing Engine becomes the master.

You can configure the broadband gateway so that the standby Routing Engine automatically becomes the master if it stops receiving keepalive signals from the original master. You can also configure automatic switchover for other problems on the master, such as a hard disk failure. For more information, see the section about Routing Engine redundancy in the *Junos OS System Basics Configuration Guide*.

Session DPC Redundancy

The MobileNext Broadband Gateway chassis includes a number of session DPCs (we recommend at least two). Each session DPC consists of two services PICs: services PIC 0 (SP0) and services PIC 1 (SP1). The session DPCs anchor control plane functions on the broadband gateway. The anchor DPC can be an individual PIC or aggregate.

The session DPCs support 1:1 redundancy. That is, the PICs in the session DPCs are configured in a one-to-one correspondence with their backups. So, for example, if the PIC0 in the session DPC in FPC slot 0 is paired with PIC0 in the session DPC in FPC slot 1, one PIC will back up the other PIC. These pairs are called aggregate multiservices (**ams-**) DPCs. However, the standby device is lost as a services DPC and all services are supplied by the active DPC PIC. In this case, the session DPC PICs associate **ams-0/0/0** and **ams-1/0/0**. You also configure units for AMS interfaces, and these are used for AAA and charging.



NOTE: You cannot configure a services PIC logical interface (`ms-0/0/0.0`, for example) if you also make the same logical interface part of an AMS group (`ams-0/0/0.0` for example). This configuration will not commit.

You configure the AMS member interface that is the preferred backup.

Interface Redundancy

The MobileNext Broadband Gateway chassis includes a number of interface Packet Forwarding Engines housed on DPCs or MPCs (we recommend at least two DPCs or MPCs). Each Packet Forwarding Engine consists of two or four Packet Forwarding Engines, depending on the DPC or MPC type. These are PFE0 and PFE1 (or optionally, PFE2 and PFE3). Some Packet Forwarding Engines are designated as anchor devices, and keep various parameters for the data plane traffic flow. Packets related to a particular flow must be processed by an anchor Packet Forwarding Engine. The anchor Packet Forwarding Engine can be a single Packet Forwarding Engine or an aggregate.

The interface Packet Forwarding Engines offer N:1 redundancy. That is, a configured number of interface Packet Forwarding Engines (N) are backed up by one warm standby Packet Forwarding Engine. Optionally, you can group Packet Forwarding Engines for redundancy purposes so that each member of the group shares the same fate.

To configure redundancy, you select a list of interface Packet Forwarding Engines to place on the active (primary) list. Then you select a different Packet Forwarding Engine to act as the secondary (standby) Packet Forwarding Engine for all Packet Forwarding Engines in the active group.

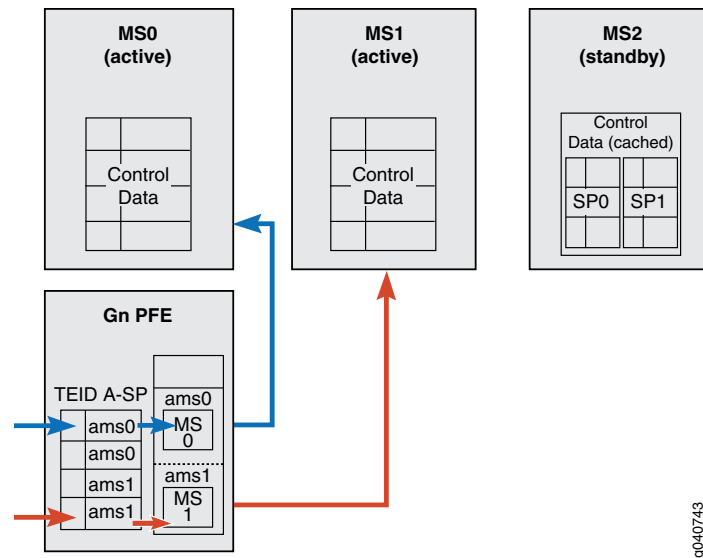
Related Documentation

- [Configuring Session DPC Redundancy on page 13](#)
- [Configuring Interface Redundancy on page 15](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 7](#)
- [Example: Configuring Broadband Gateway Redundancy on page 17](#)
- [Configuring Anchor Session DPCs and PFEs](#)

Understanding the Broadband Gateway Anchor Failover Behavior

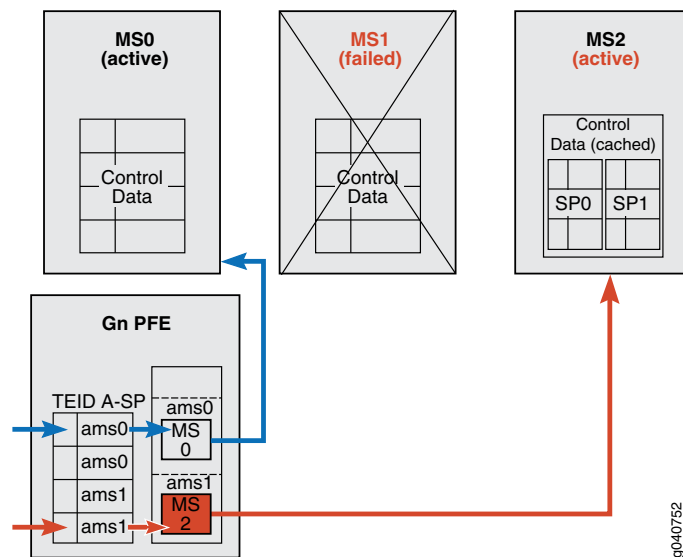
The MobileNext Broadband Gateway anchor session Dense Port Concentrators (DPCs) (housing PICs) and interface PFEs can be configured for redundancy. However, due to the different nature of the redundancy involved, 1:1 for anchor session PICs and N:1 for anchor interface PFEs, the failover behavior is slightly different.

Figure 2: Control Plane Anchor Operation Before Failure



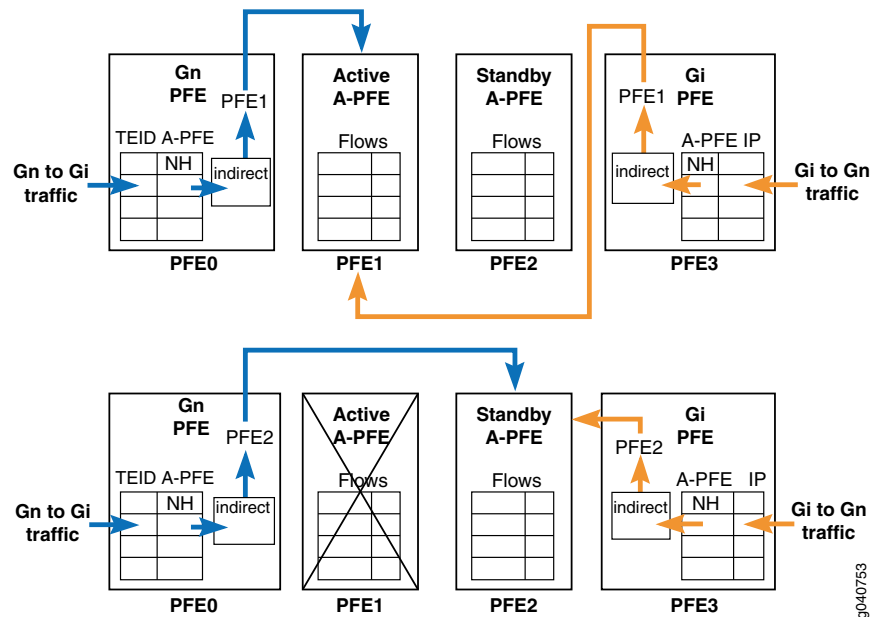
As shown in [Figure 2 on page 7](#), you can configure session DPCs with or without backup. In this case, **MS0** has no backup redundancy, while both PICs (PIC0 and PIC1) on **MS1** are backed up 1:1 by standby **MS2**. When the anchor session DPC **MS1** fails, packets cannot be processed strictly by hardware data path until the transfer of control to the new anchor is complete. This is shown in [Figure 3 on page 8](#). Note that **ams1** now points to **MS2**, the new active anchor.

Figure 3: Control Plane Anchor Operation After Failure



However, data plane packets feature N:1 anchor data path redundancy. Both pre- and post-failure Packet Forwarding Engine data paths are shown in Figure 4 on page 8. For clarity, only the active and standby Packet Forwarding Engines are shown.

Figure 4: Pre- and Post-Failure PFE Datapaths



During the transition on the ingress and egress interface Packet Forwarding Engines sending data plane packets from the failed PFE1 to the new active PFE2, packets cannot be processed strictly by hardware data path until the transfer of control to the new anchor is complete.

- Related Documentation**
- [Broadband Gateway Redundancy Overview on page 4](#)
 - [Configuring Session DPC Redundancy on page 13](#)
 - [Configuring Interface Redundancy on page 15](#)
 - [Example: Configuring Broadband Gateway Redundancy on page 17](#)
 - [Configuring Anchor Session DPCs and PFEs](#)

PART 2

Configuration

- [Configuration Tasks on page 13](#)
- [Configuration Examples on page 17](#)
- [Configuration Statements on page 21](#)

CHAPTER 2

Configuration Tasks

- [Configuring Session DPC Redundancy on page 13](#)
- [Configuring Interface Redundancy on page 15](#)

Configuring Session DPC Redundancy

The MobileNext Broadband Gateway chassis includes a number of session Dense Port Concentrators (DPCs) (we recommend at least two). Each session DPC consists of two services PICs: services PIC 0 and services PIC 1. The session DPCs anchor control plane functions on the broadband gateway.

Before you begin configuring session DPC redundancy on a broadband gateway chassis, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the session DPCs

The session DPCs support 1:1 redundancy. That is, the PICs in the session DPCs are configured in a one-to-one correspondence with their backups. So, for example, if the PICO in the session DPC in FPC slot 0 is paired with PICO in the session DPC in FPC slot 1, one PIC will back up the other PIC. These pairs are called aggregate multiservices (**ams-**) PICs and the member interfaces are called members of the AMS (**mams-**). However, the standby device is lost as a services PIC and all services are supplied by the active PIC. In this case, the session PICs associate **mams-0/0/0** and **mams-1/0/0** as active and standby pairs. You also configure units for AMS interfaces, and these are used for AAA and charging.



NOTE: You cannot configure a services PIC logical interface (**ms-0/0/0.0**, for example) if you also make the same logical interface part of an AMS (**mams-0/0/0.0**, for example). This configuration will not commit.

You configure the AMS member interface that is the preferred backup. You can configure more than one AMS group, but each must have the 1:1 redundancy, of course.

To configure AMS group membership and redundancy actions for a pair of session DPCs on a broadband gateway:

1. Configure the session DPC redundancy pair called **ams0** so that PIC 1 of the session DPC in FPC slot 0 is backed-up by FPC slot 5 PIC 1.

[edit interfaces]

```
user@host# set ams0 load-balancing-options member-interface mams-4/1/0
```

```
user@host# set ams0 load-balancing-options member-interface mams-5/1/0
```



NOTE: The `load-balancing-options` keyword has nothing to do with load balancing. When used for mobility, session DPCs automatically load-balance sessions.

2. Configure the preferred backup for **ams0** so that FPC 4 PIC 1 is the active session DPC and FPC 5 PIC 1 is the backup.

[edit interfaces]

```
user@host# set ams0 load-balancing-options high-availability-options many-to-one preferred-backup mams-5/1/0
```



NOTE: The `many-to-one` option is still used for 1:1 redundancy in this case.

3. Configure the logical interfaces (units) for **ams0** so that **unit 0** and **unit 1** are available for AAA and charging uses.

[edit interfaces]

```
user@host# set ams0 unit 1 family inet
```

```
user@host# set ams0 unit 2 family inet
```



NOTE: You do not have to assign an IP address.

4. Configure the failure parameters for the members on **ams0**.

[edit interfaces]

```
user@host# set ams0 load-balancing-options member-interface-options
```

```
redistribute-all-traffic enable-rejoin
```



NOTE: The `enable-rejoin` option is the only option currently supported for `redistribute-all-traffic`. If you configure the `redistribute-all-traffic` statement, you cannot also configure the `drop-member-traffic` statement on the same AMS group.

Related Documentation

- [Broadband Gateway Redundancy Overview on page 4](#)
- [Configuring Interface Redundancy on page 15](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 7](#)

- [Example: Configuring Broadband Gateway Redundancy on page 17](#)
- Configuring Anchor Session DPCs and PFEs

Configuring Interface Redundancy

The MobileNext Broadband Gateway chassis includes a number of interface Packet Forwarding Engines housed on Dense Port Concentrators (DPCs) or Modular Port Concentrators (MPCs) (we recommend at least two DPCs or MPCs). Each Packet Forwarding Engine consists of two or four Packet Forwarding Engines, depending on the DPC or MPC type. These are PFE0 and PFE1 (or optionally, PFE2 and PFE3). Some Packet Forwarding Engines are designated as anchor devices, and keep various parameters for the data plane traffic flow. Packets related to a particular flow must be processed by an anchor Packet Forwarding Engine.

Before you begin configuring session DPC redundancy on a broadband gateway chassis, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interface DPCs or MPCs used for mobility

The interface Packet Forwarding Engines offer N:1 redundancy. That is, a configured number of interface Packet Forwarding Engines (N) are backed up by one warm standby Packet Forwarding Engine. Optionally, you can group Packet Forwarding Engines for redundancy purposes so that each member of the group shares the same fate.

To configure interface redundancy for mobility, you select a list of interface Packet Forwarding Engines to place on the active (primary) list. Then you select a different Packet Forwarding Engine to act as the secondary (standby) Packet Forwarding Engine for all Packet Forwarding Engines in the active group.

To configure group membership and redundancy actions for a number of interface DPCs or MPCs on a broadband gateway:

1. Configure the interface DPC or MPC redundancy list called **apfe0** with all Packet Forwarding Engines in FPC slot 2 and 3 backed up in warm standby by the Packet Forwarding Engines in FPC slot 4.

[edit interfaces]

```
user@host# set apfe0 anchoring-options primary-list fpc-2
user@host# set apfe0 anchoring-options primary-list fpc-3
user@host# set apfe0 anchoring-options secondary fpc-4
user@host# set apfe0 anchoring-options warm-standby
```



NOTE: The warm-standby option is the only mode currently supported. In this configuration (for example) ge-2/0/0 is backed up by ge-4/0/0, ge-2/1/0 is backed up by ge-4/1/0, and so on.

2. Alternatively, configure the interface DPC or MPC redundancy list called **apfe1** with a Packet-Forwarding-Engine-by-Packet-Forwarding-Engine list of redundant components.

[edit interfaces]

```
user@host# set apfe1 anchoring-options primary-list pfe-7/0/0
user@host# set apfe1 anchoring-options primary-list pfe-8/0/0
user@host# set apfe1 anchoring-options secondary pfe-9/0/0
user@host# set apfe1 anchoring-options warm-standby
```



NOTE: The **warm-standby** option is the only mode currently supported. In this configuration (for example), **ge-7/0/0** or **ge-8/0/0** is backed up by **ge-9/0/0** in case of failure, but not **ge-7/1/0**.

3. Optionally, you can configure a group name for Packet-Forwarding-Engine-level redundancy **apfe1** and **apfe2** so that all components share the same fate.

[edit interfaces]

```
user@host# set apfe1 apfe-group-set apfe-group-name1
user@host# set apfe1 anchoring-options primary-list pfe-7/0/0
user@host# set apfe1 anchoring-options primary-list pfe-8/0/0
user@host# set apfe1 anchoring-options secondary pfe-9/0/0
user@host# set apfe1 anchoring-options warm-standby
user@host# set apfe2 apfe-group-set apfe-group-name1
user@host# set apfe2 anchoring-options primary-list pfe-7/2/0
user@host# set apfe2 anchoring-options primary-list pfe-8/2/0
user@host# set apfe2 anchoring-options secondary pfe-9/2/0
user@host# set apfe2 anchoring-options warm-standby
```

Related Documentation

- [Broadband Gateway Redundancy Overview on page 4](#)
- [Configuring Session DPC Redundancy on page 13](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 7](#)
- [Example: Configuring Broadband Gateway Redundancy on page 17](#)
- [Configuring Anchor Session DPCs and PFEs](#)

CHAPTER 3

Configuration Examples

- [Example: Configuring Broadband Gateway Redundancy on page 17](#)

Example: Configuring Broadband Gateway Redundancy

This example shows how to configure redundancy for a MobileNext Broadband Gateway chassis containing session Dense Port Concentrators (DPCs) and interface DPCs and Module Port Concentrators (MPCs) (housing Packet Forwarding Engines). Routing Engine redundancy is not unique to mobility and is not discussed in this example. This topic describes only the unique mobile redundancy portion of the configuration.

- [Requirements on page 17](#)
- [Overview on page 17](#)
- [Configuration on page 18](#)
- [Verification on page 20](#)

Requirements

This example uses the following hardware and software components:

- An MX chassis equipped with four session DPCs and three interface DPCs or MPCs.
- Junos OS Mobility package

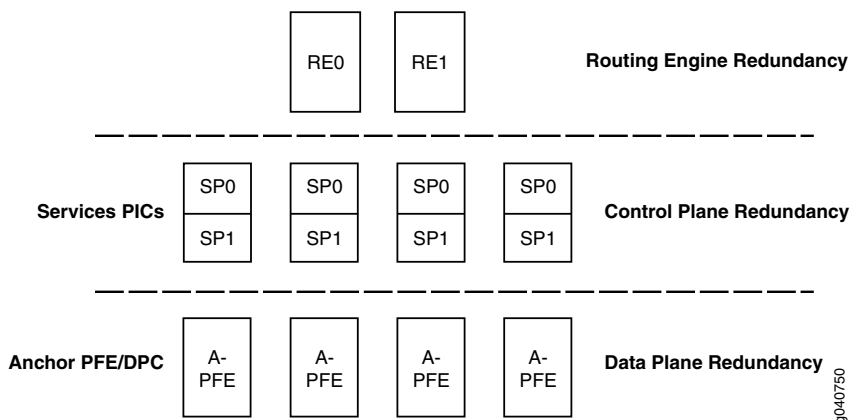
Before you begin:

- Install the chassis hardware.
- Configure the chassis.

Overview

[Figure 5 on page 18](#) shows a broadband gateway chassis with multiple Routing Engines (not discussed further in this example), session DPCs, and interfaces Packet Forwarding Engines (housed in DPCs or MPCs).

Figure 5: Redundancy Example for the Broadband Gateway



In this example, the chassis has session DPCs in Packet Forwarding Engines slots 4 and 5 featuring 1:1 redundancy. Group **ams0** will backup PIC **mams-4/1/0** with **mams-5/1/0** and redistribute all traffic with the rejoin option. Group **ams1** will back up PIC **mams-4/0/0** with **mams-5/0/0**. Both groups have two logical units for authentication, authorization, and accounting (AAA) and charging. The chassis also has interface DPCs or MPCs in Packet Forwarding Engines slots 7, 8, and 9, featuring N:1 redundancy, in this case, 2:1. This example backs up Packet Forwarding Engines **pfe-7/0/0** and **pfe-8/0/0** with warm standby **pfe-9/0/0**.

Configuration

Redundancy for the above is configured by:

- [Configuration on page 18](#)

Configuration

CLI Quick Configuration

```
[edit interfaces]
user@host# set ams0 load-balancing-options member-interface mams-4/1/0
user@host# set ams0 load-balancing-options member-interface mams-5/1/0
user@host# set ams0 load-balancing-options high-availability-options many-to-one
preferred-backup mams-5/1/0
user@host# set ams0 load-balancing-options member-interface-options
redistribute-all-traffic enable-rejoin
user@host# set ams0 unit 1 family inet
user@host# set ams0 unit 2 family inet
user@host# set ams1 load-balancing-options member-interface mams-4/0/0
user@host# set ams1 load-balancing-options member-interface mams-5/0/0
user@host# set ams1 load-balancing-options high-availability-options many-to-one
preferred-backup mams-5/0/0
user@host# set ams1 unit 1 family inet
user@host# set ams1 unit 2 family inet

user@host#set apfe0 anchoring-options primary-list pfe-7/0/0
user@host#set apfe0 anchoring-options primary-list pfe-8/0/0
user@host#set apfe0 anchoring-options secondary pfe-9/0/0 warm-standby
```

Results From configuration mode, confirm your configuration by entering the **show interfaces** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** command output includes only the configuration statements that are relevant to this example.

```
ams0 {
  load-balancing-options {
    member-interface mams-4/1/0;
    member-interface mams-5/1/0;
    member-failure-options {
      redistribute-all-traffic {
        enable-rejoin;
      }
    }
    high-availability-options {
      many-to-one {
        preferred-backup mams-5/1/0;
      }
    }
  }
  unit 1 {
    family inet;
  }
  unit 2 {
    family inet;
  }
}
ams1 {
  load-balancing-options {
    member-interface mams-4/0/0;
    member-interface mams-5/0/0;
    member-failure-options {
      drop-member-traffic {
        rejoin-timeout 10000;
      }
    }
    high-availability-options {
      many-to-one {
        preferred-backup mams-5/1/0;
      }
    }
  }
  unit 1 {
    family inet;
  }
  unit 2 {
    family inet;
  }
}

apfe0 {
  anchoring-options {
    primary-list {
```

```
fpc-7/0/0;  
fpc-8/0/0;  
}  
secondary pfe-9/0/0;  
warm-standby;  
}  
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Redundancy

Purpose Verify that redundancy is enabled or not.

Action From operational mode, enter the **show unified-edge ggsn-pgw interfaces redundancy** command.



.....
NOTE: To view failover statistics, enter the **show unified-edge ggsn-pgw exception-handling statistics failover** command.
.....

Meaning The output shows the redundancy parameters or failover statistics configured on the gateway

Related Documentation

- [Broadband Gateway Redundancy Overview on page 4](#)
- [Configuring Session DPC Redundancy on page 13](#)
- [Configuring Interface Redundancy on page 15](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 7](#)
- [Configuring Anchor Session DPCs and PFEs](#)

CHAPTER 4

Configuration Statements

- [\[edit interfaces amsx\] Hierarchy Level on page 21](#)
- [\[edit interfaces apfe\] Hierarchy Level on page 22](#)

[\[edit interfaces amsx\] Hierarchy Level](#)

```
interfaces amsx {  
  hold-time {  
    ...  
  }  
  layer2-policer {  
    ...  
  }  
  load-balancing-options {  
    high-availability-options {  
      many-to-one {  
        preferred-backup preferred-backup;  
      }  
    }  
    member-failure-options {  
      drop-member-traffic {  
        enable-rejoin;  
        rejoin-timeout rejoin-timeout;  
      }  
      redistribute-all-traffic {  
        enable-rejoin;  
      }  
    }  
    member-interface interface-name;  
  }  
  multi-chassis-protection {  
    ...  
  }  
  services-options {  
    ...  
  }  
  traceoptions {  
    ...  
  }  
  unit interface-unit-number {  
    dial-options {  
      (dedicated | shared);  
    }  
  }  
}
```

```
    ipsec-interface-id ipsec-interface-id;  
  }  
  family family;  
  load-balancing-options {  
    preferred-active interface-name;  
  }  
}  
}
```

Related
Documentation

- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit interfaces apfe] Hierarchy Level

```
interfaces apfe {  
  anchoring-options {  
    apfe-group-set apfe-group-set;  
    primary-list {  
      [anchoring-device-name];  
    }  
    secondary anchoring-device-name;  
    warm-standby;  
  }  
  hold-time {  
    ...  
  }  
  layer2-policer {  
    ...  
  }  
  multi-chassis-protection {  
    ...  
  }  
  traceoptions {  
    ...  
  }  
}
```

Related
Documentation

- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

pfes

Syntax	pfes { [interface <i>interface-name</i>]; }
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system], [edit unified-edge gateways sgw <i>gateway-name</i> system]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> system] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify the interfaces used for anchoring subscribers in the Packet Forwarding Engine in the broadband gateway. The remaining statements are explained separately.
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring Anchor Session DPCs and PFEs system (MobileNext Broadband Gateway Interfaces) on page 61


service-pics

Syntax	service-pics { [interface <i>interface-name</i>]; }
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify the interfaces used for anchoring mobile subscriber-aware services in the broadband gateway. The remaining statements are explained separately.
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> system (MobileNext Broadband Gateway Interfaces) on page 61

session-pics

Syntax	<pre>session-pics { [interface <i>interface-name</i>]; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system], [edit unified-edge gateways sgw <i>gateway-name</i> system]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> system] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify the interfaces used for the mobile control plane in the broadband gateway. The remaining statements are explained separately.
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring Anchor Session DPCs and PFEssystem (MobileNext Broadband Gateway Interfaces) on page 61

apfe-group-set (Aggregated Packet Forwarding Engine)

Syntax	<code>apfe-group-set <i>apfe-group-set</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> anchoring-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify that the anchor Packet Forwarding Engines belonging to the FPCs configured for redundancy should belong to an aggregated Packet Forwarding Engine (apfe) group set. When you specify an apfe group set, the FPCs configured on the different apfe interfaces share the same fate.</p> <p>For example, you configure two apfe interfaces: apfe0 and apfe1. This means that if an anchor Packet Forwarding Engine on an FPC in apfe0 switches to the corresponding backup anchor Packet Forwarding Engine on the backup FPC, then the anchor Packet Forwarding Engine on the corresponding FPC in apfe1 also switches to the corresponding backup anchor Packet Forwarding Engine on the backup FPC.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>NOTE: The apfe-group-set is configured at the apfe level. Since the apfe interfaces have Packet Forwarding Engine interfaces (pfe-) as their members, the apfe-group-set configuration groups interfaces at the Packet Forwarding Engine level rather than at the FPC level.</p> </div>
Default	If you do not configure the apfe-group-set statement, then the apfe interface that you configure behaves as a standalone entity and it is not influenced by other apfe interfaces configured on the broadband gateway.
Options	<p><i>apfe-group-set</i>—Name of the apfe group set.</p> <p>Range: Up to 32 characters</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • anchoring-options (Aggregated Packet Forwarding Engine) on page 26 • Configuring Interface Redundancy on page 15 • Example: Configuring Broadband Gateway Redundancy on page 17

anchoring-options (Aggregated Packet Forwarding Engine)

Syntax	<pre>anchoring-options { apfe-group-set apfe-group-set; primary-list { [anchoring-device-name]; } secondary anchoring-device-name; warm-standby; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the options for the anchor Packet Forwarding Engine redundancy. The redundancy options are configured at the level of the Flexible PIC Concentrator (FPC). The FPCs that are configured for redundancy must be of the same type—that is, they must have the same number of Packet Forwarding Engines and the same forwarding capabilities.</p> <p>The type of redundancy supported is many-to-one (N:1), which means that one Packet Forwarding Engine acts as the backup for one or more (N) Packet Forwarding Engines. When you configure FPCs for anchor Packet Forwarding Engine redundancy, the corresponding anchor Packet Forwarding Engines in each FPC are configured for N:1 redundancy. The first Packet Forwarding Engine of each primary FPC is backed up by the first Packet Forwarding Engine of the backup FPC, the second Packet Forwarding Engine of each primary FPC is backed up by the second Packet Forwarding Engine of the backup FPC, and so on.</p> <p>For example, consider the case when you configure three FPCs—FPC1, FPC2, and FPC3—for redundancy with FPC1 and FPC2 as primary members, and FPC3 as backup. If each FPC has two Packet Forwarding Engines (PFE0 and PFE1), then FPC1-PFE0 and FPC2-PFE0 are backed up by FPC3-PFE0. Similarly, FPC1-PFE1 and FPC2-PFE1 are backed up by FPC3-PFE1.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Interface Redundancy on page 15• Configuring Interface DPCs or MPCs for User Mobility Traffic• Example: Configuring Broadband Gateway Redundancy on page 17• interfaces (Aggregated Packet Forwarding Engine) on page 43


dedicated (IPsec)

Syntax	<code>dedicated;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i> dial-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify that Dynamic End Point (DEP) IP Security (IPsec) tunnels are supported in dedicated logical interface (ifl) mode for the aggregated multiservices (AMS) interface. In dedicated ifl mode, each DEP IPsec tunnel is mapped to one AMS ifl .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • dial-options (IPsec) on page 27 • shared (IPsec) on page 61

dial-options (IPsec)

Syntax	<pre>dial-options { (dedicated shared); ipsec-interface-id <i>ipsec-interface-id</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure the parameters to support Dynamic End Point (DEP) IP Security (IPsec) tunnels on the aggregated multiservices (AMS) interface. DEP IPsec tunnels are supported in two modes: dedicated logical interface (ifl) mode and shared ifl mode.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • unit (Aggregated Multiservices) on page 62

drop-member-traffic (Aggregated Multiservices)

Syntax	<pre>drop-member-traffic { enable-rejoin; rejoin-timeout <i>rejoin-timeout</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify whether the broadband gateway should drop traffic to a multiservices PIC when it fails.</p> <ul style="list-style-type: none"> For one-to-one (1:1) mobile control plane redundancy, this configuration is valid only when both multiservices PICs have failed. For many-to-one (N:1) high availability (HA) for service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall), this configuration is valid only when two or more multiservices PICs have failed. <p>The remaining statements are explained separately.</p> <div style="margin-top: 10px;">  <p>NOTE: If you configure the drop-member-traffic statement, then you cannot configure the redistribute-all-traffic statement; that is, they are mutually exclusive.</p> </div>
Default	If this statement is not configured, then the default behavior is to drop member traffic with a rejoin timeout of 120 seconds. If the member does not come back online within this time, then it must be manually brought back into the AMS interface, using the request interface load-balancing revert command.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Session DPC Redundancy on page 13 • Example: Configuring Broadband Gateway Redundancy on page 17 • member-failure-options (Aggregated Multiservices) on page 49 • request interface load-balancing revert (Aggregated Multiservices) on page 68

egress-key (Aggregated Multiservices)

Syntax	<code>egress-key (destination-ip source-ip);</code>
Hierarchy Level	[edit services service-set <i>service-set-name</i> interface-service load-balancing-options hash-keys]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the hash keys to be used in the egress flow direction. The configuration is mandatory if you are using AMS for Network Address Translation (NAT). This configuration is not mandatory if you are using AMS for stateful firewall; if the hash keys are not configured, then the defaults are chosen. (See hash-keys (Aggregated Multiservices) for more information.)
Options	<p>The following hash keys can be configured in the egress direction:</p> <p>destination-ip—Use the destination IP address of the flow to compute the hash used in load balancing.</p> <p>source-ip—Use the source IP address of the flow to compute the hash used in load balancing.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • hash-keys (Aggregated Multiservices) on page 32

enable-rejoin (Aggregated Multiservices)

Syntax	enable-rejoin;
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options drop-member-traffic], [edit interfaces <i>interface-name</i> load-balancing-options member-failure-options redistribute-all-traffic]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support for the [edit interfaces <i>interface-name</i> load-balancing-options member-failure-options drop-member-traffic] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Enable the failed member to rejoin the aggregated multiservices (AMS) interface after the member comes back online.</p> <ul style="list-style-type: none">• For one-to-one (1:1) mobile control plane redundancy, this configuration is used in case both members fail, and it allows the members to rejoin the ams interface automatically.• For many-to-one (N:1) high availability (HA) for service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall), 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. For this reason, the inactive member cannot be the backup for the active member (even after it comes back online) unless the request interface load-balancing revert command is explicitly issued to return the inactive member to the active state.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Session DPC Redundancy on page 13• drop-member-traffic (Aggregated Multiservices) on page 28• Example: Configuring Broadband Gateway Redundancy on page 17• redistribute-all-traffic (Aggregated Multiservices) on page 55• request interface load-balancing revert (Aggregated Multiservices) on page 68

family (Aggregated Multiservices)

Syntax	<code>family <i>family</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure protocol family information for the logical interface.
Options	<i>family</i> —Protocol family. Currently, only one option, inet (IP version 4 suite), is supported.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Session DPC Redundancy on page 13• Example: Configuring Broadband Gateway Redundancy on page 17• unit (Aggregated Multiservices) on page 62

hash-keys (Aggregated Multiservices)

Syntax	<pre>hash-keys { egress-key (destination-ip source-ip); ingress-key (destination-ip source-ip); resource-triggered; }</pre>
Hierarchy Level	[edit services service-set <i>service-set-name</i> interface-service load-balancing-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the hash keys used for load balancing in aggregated multiservices (AMS) for service applications (Network Address Translation [NAT], stateful firewall, application-level gateway [ALG], HTTP header enrichment, and mobility). The hash keys supported in the ingress and egress direction are the source IP address and destination IP address.</p> <p>Hash keys are used to define the load-balancing behavior among the various members in the AMS group. For example, if hash-keys is configured as source-ip, then the hashing would be performed based on the source IP address of the packet. Therefore, all packets with the same source IP address land on the same member. Hash keys must be configured with respect to the traffic direction: ingress or egress. For example, if hash-keys is configured as source-ip in the ingress direction, then it should be configured as destination-ip in the egress direction. This is required to ensure that the packets of the same flow reach the same member of the AMS group.</p> <p>The configuration of the ingress and egress hash keys is mandatory if you are using AMS for NAT. This configuration is not mandatory if you are using AMS for stateful firewall; if the hash keys are not configured, then the defaults are chosen. Refer to Table 3 on page 33 for the supported hash keys.</p> <p>The resource-triggered option enables anchor session PICs to use the load or resource information from the anchor services PICs to select the AMS member will anchor the services for the subscriber for load balancing among AMS members. In addition, for mobile subscriber-aware services (such as HTTP header enrichment), you must configure the resource-triggered statement, which means that the load balancing is not done using the ingress and egress keys.</p>

Table 3: Hash Keys Supported for AMS for Service Applications

Service Set at Ingress Interface			Service Set at Egress Interface	
Hash Keys for NAT				
NAT Type	Ingress hash key	Egress hash key	Ingress hash key	Egress hash key
source static	Destination IP address	Source IP address	Source IP address	Destination IP address
source dynamic	Source IP address	Destination IP address	Destination IP address	Source IP address
Network Address Port Translation (NAPT)	Source IP address	Destination IP address	Destination IP address	Source IP address
destination static	Source IP address	Destination IP address	Destination IP address	Source IP address
Hash Keys for Stateful Firewall				
Stateful Firewall	Destination IP address	Source IP address	Destination IP address	Source IP address
Stateful Firewall	Source IP address	Destination IP address	Source IP address	Destination IP address



NOTE: If NAT is used in the service set (along with stateful firewall and ALG), then the hash keys should be based on the NAT type; otherwise, the hash keys of the stateful firewall should be used.

The remaining statements are explained separately.

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

Related Documentation • [load-balancing-options \(Aggregated Multiservices for Services Applications\) on page 46](#)

high-availability-options (Aggregated Multiservices)

Syntax high-availability-options {
 many-to-one {
 preferred-backup *preferred-backup*;
 }
 }

Hierarchy Level [edit interfaces *interface-name* load-balancing-options]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

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

- For one-to-one (1:1) mobile control plane redundancy, the preferred backup multiservices PIC, in hot standby mode, backs up one multiservices PIC.
- For many-to-one (N:1) high availability support for service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall), the preferred backup multiservices PIC, in hot standby mode, backs up one or more (N) active multiservices PICs.



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

The remaining statements are explained separately.



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

Related Documentation • [Configuring Session DPC Redundancy on page 13](#)
 • [Example: Configuring Broadband Gateway Redundancy on page 17](#)
 • [load-balancing-options \(Aggregated Multiservices\) on page 45](#)

ingress-key (Aggregated Multiservices)


Syntax	ingress-key (destination-ip source-ip);
Hierarchy Level	[edit services service-set <i>service-set-name</i> interface-service load-balancing-options hash-keys]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the hash keys to be used in the ingress flow direction. The configuration is mandatory if you are using AMS for Network Address Translation (NAT). This configuration is not mandatory if you are using AMS for stateful firewall; if the hash keys are not configured, then the defaults are chosen.
Options	<p>The following hash keys can be configured in the ingress direction:</p> <p>destination-ip—Use the destination IP address of the flow to compute the hash used in load balancing.</p> <p>source-ip—Use the source IP address of the flow to compute the hash used in load balancing.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • hash-keys (Aggregated Multiservices) on page 32

interface (Packet Forwarding Engine)

Syntax	[interface <i>interface-name</i>];
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system pfes], [edit unified-edge gateways sgw <i>gateway-name</i> system pfes]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> system pfes] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the interface representing the Packet Forwarding Engine used for anchoring subscribers in the broadband gateway. The following conditions are applicable to the Packet Forwarding Engine interfaces configured here:</p> <ul style="list-style-type: none"> The aggregated Packet Forwarding Engine interfaces (apfe) specified in this statement must already be defined at the [edit interfaces] hierarchy level. For a broadband gateway configured as a gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW), the Packet Forwarding Engine interfaces must have mobility ggsn-pgw as their forwarding package at [edit chassis fpc <i>fpc-slot</i> pfe <i>pfe-id</i> forwarding-packages] hierarchy level. <p> NOTE: If the specified Packet Forwarding Engine interface is an apfe interface, then all the member interfaces of the apfe interface must have mobility ggsn-pgw as their forwarding package (at the [edit chassis fpc <i>fpc-slot</i> pfe <i>pfe-id</i> forwarding-packages] hierarchy level).</p> <ul style="list-style-type: none"> For a broadband gateway configured as a Serving Gateway (S-GW), the Packet Forwarding Engine interfaces must have mobility sgw as their forwarding package at the [edit chassis fpc <i>fpc-slot</i> pfe <i>pfe-id</i> forwarding-packages] hierarchy level. <p> NOTE: If the specified Packet Forwarding Engine interface is an apfe interface, then all member interfaces of the apfe interface must have mobility sgw as their forwarding package (at the [edit chassis fpc <i>fpc-slot</i> pfe <i>pfe-id</i> forwarding-packages] hierarchy levels).</p> <ul style="list-style-type: none"> If a Packet Forwarding Engine interface is a member of an apfe interface, then that interface cannot be specified here. For example, if pfe-2/0/0 is a member interface of apfe interface apfe0, then pfe-2/0/0 cannot be directly specified here.
Options	<p>interface-name—Name of the interface representing the Packet Forwarding Engine.</p> <p>Syntax: The interface must be a valid Packet Forwarding Engine interface (apfe or pfe-); for example, apfe0 or pfe-1/0/0.</p>

Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• pfes on page 23• Configuring Interface Redundancy on page 15• Configuring Interface DPCs or MPCs for User Mobility Traffic• Example: Configuring Broadband Gateway Redundancy on page 17• show unified-edge ggsn-pgw system interfaces on page 110• show unified-edge sgw system interfaces on page 112


interface (Services PIC)

Syntax	[interface <i>interface-name</i>];
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system service-pics]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the interface representing the services PIC used for anchoring services-related subscriber sessions in the broadband gateway. The following conditions are applicable to the services PIC interfaces configured here:</p> <ul style="list-style-type: none"> • The aggregated multiservices interfaces (ams) specified in this statement must already be defined at the [edit interfaces] hierarchy level. • The services PIC must have the jservices-hcm, jservices-mss, and jservices-crypto-base packages configured at the [edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider] hierarchy level. • If a services PIC interface is a member of an aggregated multiservices interface, then that member interface cannot be specified here. For example, if mams-2/0/0 is a member interface of the aggregated multiservices interface ams0, then ms-2/0/0/ cannot be directly specified here.
	<div>  <p>NOTE: If an aggregated multiservices interface (for example ams0) is used for HTTP header enrichment, then load balancing is performed to anchor subscriber-aware services in one of the member interfaces. Otherwise, load balancing is not performed.</p> </div>
Options	<p>interface-name—Name of the interface representing the services PIC.</p> <p>Syntax: The interface must be a valid multiservices interface (ams or ms-a/b/0, where a is the Flexible PIC Concentrator [FPC] slot number and b is the PIC slot number); for example, ams0 or ms-1/0/0.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring the MobileNext Broadband Gateway Chassis • service-pics on page 23 • show unified-edge ggsn-pgw system interfaces on page 110

interface (Session PIC)

Syntax	<code>[interface <i>interface-name</i>];</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system session-pics]</code> , <code>[edit unified-edge gateways sgw <i>gateway-name</i> system session-pics]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the <code>[edit unified-edge gateways sgw <i>gateway-name</i> system session-pics]</code> hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the interface representing the session PIC used for the mobile control plane in the broadband gateway. The following conditions are applicable to the session PIC interfaces configured here:</p> <ul style="list-style-type: none"> • The aggregated multiservices interfaces (ams) specified in this statement must already be defined at the <code>[edit interfaces]</code> hierarchy level. • The session PIC must have the jservices-mobile package configured at the <code>[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> adaptive-services service-package extension-provider]</code> hierarchy level. • If a session PIC interface is a member of an aggregated multiservices interface, then that member interface cannot be specified here. For example, if mams-2/0/0 is a member interface of the aggregated multiservices interface ams0, then ms-2/0/0/ cannot be directly specified here.
Options	<p><i>interface-name</i>—Name of the interface representing the session PIC.</p> <p>Syntax: The interface must be a valid multiservices interface (ams or ms-a/b/0, where a is the Flexible PIC Concentrator [FPC] slot number and b is the PIC slot number); for example, ams0 or ms-1/0/0.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Anchor Session DPCs and PFEs • session-pics on page 24 • show unified-edge ggsn-pgw system interfaces on page 110 • show unified-edge sgw system interfaces on page 112

interface-service (Aggregated Multiservices)

Syntax	<pre> interface-service { load-balancing-options { hash-keys { egress-key (destination-ip source-ip); ingress-key (destination-ip source-ip); resource-triggered; } } service-interface <i>interface-name.unit-number</i>; } </pre>
Hierarchy Level	[edit services service-set <i>service-set-name</i>]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Support for aggregated multiservices (AMS) interfaces introduced in Junos OS Mobility Release 11.2W.</p>
Description	<p>Specify the interface name and unit number to be used in aggregated multiservices (AMS) with high availability (HA) for service applications (Network Address Translation [NAT], stateful firewall, application-level gateway [ALG], HTTP header enrichment, and mobility), and configure the load-balancing options in AMS with high availability for service applications.</p>
Options	<p>service-interface <i>interface-name.unit-number</i>—Name and unit number of the AMS interface; for example, ams0.1, where ams0 is the interface and 1 is the unit number.</p>
	<div>  <p>NOTE: Unit 0 is reserved and cannot be configured under the AMS interface.</p> </div>
	<p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> service-set (Aggregated Multiservices) on page 59

interfaces (Aggregated Multiservices)

```
Syntax  interfaces interface-name {
        load-balancing-options {
            high-availability-options {
                many-to-one {
                    preferred-backup preferred-backup;
                }
            }
            member-failure-options {
                drop-member-traffic {
                    enable-rejoin;
                    rejoin-timeout rejoin-timeout;
                }
                redistribute-all-traffic {
                    enable-rejoin;
                }
            }
        }
        member-interface interface-name;
    }
    unit interface-unit-number {
        dial-options {
            (dedicated | shared);
            ipsec-interface-id ipsec-interface-id;
        }
        family family;
        load-balancing-options {
            preferred-active interface-name;
        }
    }
}
```

Hierarchy Level [\[edit\]](#)

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the aggregated multiservices (AMS) interface. The AMS interface provides the infrastructure for load balancing and high availability (HA).

The high availability feature is used for mobile control plane redundancy and for service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall). The load-balancing feature is currently used only for service applications. For service applications, load balancing can be used with or without high availability. Mobile control plane load balancing is done by the ingress Packet Forwarding Engine.



NOTE: The interfaces must be valid aggregated multiservices interfaces (ams); for example, ams0 or ams1, and so on. The ams infrastructure is supported only in chassis with Trio-based modules and Multiservices Dense Port Concentrators (MS-DPCs).

The remaining statements are explained separately.

Options	interface-name —Name of the aggregated multiservices interface (ams); for example, ams0 or ams1 , and so on.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Session DPC Redundancy on page 13• Example: Configuring Broadband Gateway Redundancy on page 17

interfaces (Aggregated Packet Forwarding Engine)

Syntax `interfaces interface-name {
 anchoring-options {
 apfe-group-set apfe-group-set;
 primary-list {
 [anchoring-device-name];
 }
 secondary anchoring-device-name;
 warm-standby;
 }
}`

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the aggregated Packet Forwarding Engine interface (**apfe**) used for anchor Packet Forwarding Engine redundancy on the broadband gateway.

The type of redundancy supported is many-to-one (N:1), which means that one Packet Forwarding Engine acts as the backup for one or more (N) Packet Forwarding Engines. When you configure Flexible PIC Concentrators (FPCs) for anchor Packet Forwarding Engine redundancy, the corresponding anchor Packet Forwarding Engines in each FPC are configured for N:1 redundancy. The first Packet Forwarding Engine of each primary FPC is backed up by the first Packet Forwarding Engine of the backup FPC, the second Packet Forwarding Engine of each primary FPC is backed up by the second Packet Forwarding Engine of the backup FPC, and so on.



NOTE: The interfaces must be valid **apfe** interfaces; for example, **apfe0** or **apfe1**.

The remaining statements are explained separately.

Options **interface-name**—Name of the aggregated Packet Forwarding Engine interface (**apfe**); for example, **apfe0** or **apfe1**, and so on.

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

Related Documentation

- [Configuring Interface Redundancy on page 15](#)
- [Example: Configuring Broadband Gateway Redundancy on page 17](#)

ipsec-interface-id (IPsec)

Syntax	<code>ipsec-interface-id <i>ipsec-interface-id</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i> dial-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the IP Security (IPsec) interface identifier for a group of Dynamic End Point (DEP) peers.
Options	<i>ip-sec-interface-id</i> —IPsec interface identifier. Range: 1 through 63 characters
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• dial-options (IPsec) on page 27

load-balancing-options (Aggregated Multiservices)

Syntax

```
load-balancing-options {
  high-availability-options {
    many-to-one {
      preferred-backup preferred-backup;
    }
  }
  member-failure-options {
    drop-member-traffic {
      enable-rejoin;
      rejoin-timeout rejoin-timeout;
    }
    redistribute-all-traffic {
      enable-rejoin;
    }
  }
  member-interface interface-name;
}
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

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

The following modes of high availability are supported with AMS:

- One-to-one (1:1) mobile control plane redundancy—In this case, one active multiservices PIC is backed up by one standby multiservices PIC in hot standby mode.
- Many-to-one (N:1) high availability for service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall)—In this case, one multiservices PIC is the backup (in hot standby mode) for one or more (N) active multiservices PICs. If one of the active multiservices PICs goes down, then the backup replaces it as the active multiservices PIC. When the failed PIC comes back online, it becomes the new backup. This is called floating backup mode.



NOTE: In hot standby mode, the operational state of subscribers anchored on the active multiservices PIC (or PICs) is actively synchronized with the standby multiservices PIC.

The remaining statements are explained separately.

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

- Related Documentation**
- [Configuring Session DPC Redundancy on page 13](#)
 - [Example: Configuring Broadband Gateway Redundancy on page 17](#)
 - [interfaces \(Aggregated Multiservices\) on page 41](#)


load-balancing-options (Aggregated Multiservices for Services Applications)

Syntax	<pre>load-balancing-options { hash-keys { egress-key (destination-ip source-ip); ingress-key (destination-ip source-ip); resource-triggered; } }</pre>
Hierarchy Level	[edit services service-set <i>service-set-name</i> interface-service]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the load-balancing options for aggregated multiservices (AMS) in service applications (Network Address Translation [NAT], stateful firewall, application-level gateway [ALG], HTTP header enrichment, and mobility). AMS for service applications can be used for load balancing with or without high availability (HA). Currently, load balancing is based on the configured hash keys.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	• interface-service (Aggregated Multiservices) on page 40

load-balancing-options (IPsec)

Syntax	load-balancing-options { preferred-active <i>interface-name</i> ; }
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the preferred active member to be used for load balancing the Dynamic End Point (DEP) IP Security (IPsec) tunnels on the aggregated multiservices (AMS) interface. The DEP IPsec tunnels are distributed across the members configured for the AMS interface. However, the active next hop corresponds only to the preferred active member configured here. All other next hops are on standby and no traffic is directed to those members.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • unit (Aggregated Multiservices) on page 62

many-to-one (Aggregated Multiservices)

Syntax	many-to-one { preferred-backup <i>preferred-backup</i> ; }
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options high-availability-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the initial preferred backup for the aggregated multiservices (AMS) interface.
	<div>  <p>NOTE: The preferred backup must be one of the member interfaces (<i>mams-</i>) that have already been configured at the [edit interfaces <i>interface-name</i> 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.</p> </div> <p>The remaining statements are explained separately.</p>
Options	preferred-backup <i>preferred-backup</i> —Name of the preferred backup member interface. The member interface format is mams-a/b/0 , where a is the Flexible PIC Concentrator (FPC) slot number and b is the PIC slot number.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Session DPC Redundancy on page 13 • Example: Configuring Broadband Gateway Redundancy on page 17 • high-availability-options (Aggregated Multiservices) on page 34

member-failure-options (Aggregated Multiservices)

Syntax

```
member-failure-options {
  drop-member-traffic {
    enable-rejoin;
    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 Mobility Release 11.2W.

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 4 on page 49 displays the behavior of the member interface after the failure of the first multiservices PIC. Table 5 on page 50 displays the behavior of the member interface after the failure of two multiservices PICs.



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

Table 4: Behavior of Member Interface After One Multiservices PIC Fails

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

Table 5: Behavior of Member Interface After Two Multiservices PICs Fail

High Availability Mode	Configuration	rejoin-timeout	enable-rejoin	Behavior when member rejoins before rejoin-timeout expires	Behavior when member rejoins after rejoin-timeout expires
One-to-one (1:1) mobile control plane redundancy	drop-member-traffic	Configured	Not configured	<p>The traffic is dropped since both members are down.</p> <p>The first member to rejoin becomes the active member. The second member to rejoin becomes the backup. This behavior is handled automatically by the AMS infrastructure.</p>	<p>The traffic is dropped since both members are down. Both members are moved to the inactive state.</p> <p>An explicit request interface load-balancing revert command is required to make both members rejoin the AMS.</p>
One-to-one (1:1) mobile control plane redundancy	drop-member-traffic	Configured	Configured	<p>The traffic is dropped since both members are down. The first member to rejoin becomes the active member. The second member to rejoin becomes the backup. This behavior is handled automatically by the AMS infrastructure.</p>	<p>The traffic is dropped since both members are down. The first member to rejoin becomes the active member. The second member to rejoin becomes the backup. This behavior is handled automatically by the AMS infrastructure.</p>
One-to-one (1:1) mobile control plane redundancy	redistribute-all-traffic	Not applicable	Not configured	<p>The traffic is dropped since both members are down. Both members are moved to the inactive state.</p> <p>An explicit request interface load-balancing revert command is required to make both members rejoin the AMS.</p>	
One-to-one (1:1) mobile control plane redundancy	redistribute-all-traffic	Not applicable	Configured	<p>The traffic is dropped since both members are down.</p> <p>The first member to rejoin becomes the active member. The second member to rejoin becomes the backup. This behavior is handled automatically by the AMS infrastructure.</p>	
Many-to-one (N:1) high availability support for service applications	drop-member-traffic	Configured	Not configured	<p>The existing traffic for the second failed member is <i>not</i> redistributed to the other members. The member is moved to the discard state.</p> <p>If the member comes back up before the rejoin timeout expires, the traffic is restored to the member and the</p>	<p>The existing traffic for the second failed member is <i>not</i> redistributed to the other members.</p> <p>The first member rejoins the AMS automatically. However, the other members who are rejoining are moved to the inactive state. An explicit request interface load-balancing revert</p>

Table 5: Behavior of Member Interface After Two Multiservices PICs Fail (*continued*)

High Availability Mode	Configuration	rejoin-timeout	enable-rejoin	Behavior when member rejoins before rejoin-timeout expires	Behavior when member rejoins after rejoin-timeout expires
				member is moved to the active state.	command is required to make these members rejoin the AMS.
Many-to-one (N:1) high availability support for service applications	drop-member-traffic	Configured	Configured	<p>The existing traffic for the second failed member is not redistributed to the other members. The first member to rejoin becomes an active member.</p> <p>The second member to rejoin becomes the backup. This behavior is handled automatically by the AMS infrastructure.</p>	<p>The existing traffic for the second failed member is not redistributed to the other members until the rejoin timeout expires. Once the rejoin timeout expires, the traffic is redistributed to the other members.</p> <p>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.</p>
Many-to-one (N:1) high availability support for service applications	redistribute-all-traffic	Not applicable	Not configured	<p>The traffic is dropped since both members are down. Both members are moved to the inactive state.</p> <p>An explicit request interface load-balancing revert command is required to make both members rejoin the AMS.</p>	
Many-to-one (N:1) high availability support for service applications	redistribute-all-traffic	Not applicable	Configured	<p>Before rejoin, the traffic is redistributed to existing active members.</p> <p>After a failed member rejoins, the traffic is load-balanced again. This may impact existing traffic flows.</p>	

The remaining statements are explained separately.

Default If **member-failure-options** are not configured, then the default behavior is to drop member traffic with a rejoin timeout of 120 seconds. If the member does not come back online within this time, then it must be manually brought back into the AMS interface, using the **request interface load-balancing revert** command.

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

- Related Documentation**
- [Configuring Session DPC Redundancy on page 13](#)
 - [Example: Configuring Broadband Gateway Redundancy on page 17](#)
 - [load-balancing-options \(Aggregated Multiservices\) on page 45](#)
 - [request interface load-balancing revert \(Aggregated Multiservices\) on page 68](#)

member-interface (Aggregated Multiservices)

Syntax	<code>member-interface <i>interface-name</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the member interfaces for the aggregated multiservices (AMS) interface. You can configure multiple interfaces by specifying each interface in a separate statement.</p> <ul style="list-style-type: none"> • For mobile control plane redundancy, which supports one-to-one (1:1) redundancy, you must specify only two interfaces. • For high availability service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall) that support many-to-one (N:1) redundancy, you can specify two or more interfaces.



NOTE: The member interfaces that you specify must be members of aggregated multiservices interfaces (mams-) on the broadband gateway.



The remaining statements are explained separately.

Options	<i>interface-name</i> —Name of the member interface. The member interface format is mams-a/b/0 , where a is the Flexible PIC Concentrator (FPC) slot number and b is the PIC slot number.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Session DPC Redundancy on page 13 • Example: Configuring Broadband Gateway Redundancy on page 17 • load-balancing-options (Aggregated Multiservices) on page 45


preferred-active (IPsec)

Syntax	<code>preferred-active <i>interface-name</i>;</code>
Hierarchy Level	<code>[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i> load-balancing-options]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the preferred active member to be used for load balancing the Dynamic End Point (DEP) IP Security (IPsec) tunnels on the aggregated multiservices (AMS) interface. The following conditions are applicable for the preferred active member configured here:</p> <ul style="list-style-type: none"> • The preferred active member should already be configured as a member of the AMS interface. (To configure a member interface under AMS, use set member-interface <i>interface-name</i> at the <code>[edit interfaces <i>interface-name</i> load-balancing-options]</code> hierarchy level.) • The preferred active member must not be already configured as the preferred backup for the AMS interface. • If you configure load balancing, then the configuration of the preferred active member is mandatory.
Options	<i>interface-name</i> —Name of the member of AMS interface (mams-); for example, mams-1/0/0 .
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • load-balancing-options (IPsec) on page 47

primary-list (Aggregated Packet Forwarding Engine)

Syntax	primary-list { [<i>anchoring-device-name</i>]; }
Hierarchy Level	[edit interfaces <i>interface-name</i> anchoring-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the primary Flexible PIC Concentrators (FPCs) for the anchor Packet Forwarding Engine redundancy.
	<div>  <p>NOTE: You can configure the primary list to contain multiple FPCs. However, all the FPCs must be of the same type—that is, they should have the same number of Packet Forwarding Engines and the same forwarding capabilities.</p> </div> <p>To configure multiple primary FPCs, include the anchoring-device-name statement multiple times.</p>
Options	anchoring-device-name —Name of the FPC.
	<div>  <p>NOTE: The interface must be a valid interface (fpc-) that is defined in the broadband gateway interface hierarchy.</p> </div>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • anchoring-options (Aggregated Packet Forwarding Engine) on page 26 • Configuring Interface Redundancy on page 15 • Configuring Interface DPCs or MPCs for User Mobility Traffic • Example: Configuring Broadband Gateway Redundancy on page 17

redistribute-all-traffic (Aggregated Multiservices)

Syntax	<pre>redistribute-all-traffic { enable-rejoin; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Enable the option to redistribute traffic of a failed active member to the other active members.</p> <ul style="list-style-type: none"> For one-to-one (1:1) mobile control plane redundancy, since both members have failed, the traffic is dropped. 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. <p>The remaining statement is explained separately.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>NOTE: If you configure the <code>redistribute-all-traffic</code> statement, then you cannot configure the <code>drop-member-traffic</code> statement; that is, they are mutually exclusive.</p> </div>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Session DPC Redundancy on page 13 Example: Configuring Broadband Gateway Redundancy on page 17 member-failure-options (Aggregated Multiservices) on page 49


rejoin-timeout (Aggregated Multiservices)

Syntax	<code>rejoin-timeout <i>rejoin-timeout</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options drop-member-traffic]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the time by when a failed member should rejoin the aggregated multiservices (AMS) interface automatically. If the failed member does not rejoin by the configured time, then the member is moved to the “inactive” state and the traffic meant for this member is dropped.</p> <p>If the member does not come back online within this time, then it must be manually brought back into the AMS interface, using the request interface load-balancing revert command.</p>
Default	If you do not configure a value, the default value of 120 seconds is used.
Options	<p><i>rejoin-timeout</i>—Time, in seconds, by which a failed member must rejoin.</p> <p>Default: 120 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Session DPC Redundancy on page 13• drop-member-traffic (Aggregated Multiservices) on page 28• Example: Configuring Broadband Gateway Redundancy on page 17• request interface load-balancing revert (Aggregated Multiservices) on page 68

resource-triggered (Aggregated Multiservices)

Syntax	resource-triggered;
Hierarchy Level	[edit services service-set <i>service-set-name</i> interface-service load-balancing-options hash-keys]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify that the load balancing for aggregated multiservices (AMS) for services applications should be triggered based on the resources (load) information from the services PICs.</p> <p>If the HTTP header enrichment service is configured as a mobility subscriber-aware service, then the anchor services PIC can be configured as either a multiservices interface (for example ms-1/0/0) or an AMS interface (for example ams0). If it is configured as an AMS interface, then the load balancing must be performed by the anchor session PICs, which are configured using the resource-triggered statement. Therefore, the resource-triggered statement is mandatory for subscriber-aware services using AMS interfaces.</p> <p>Only one service set can be configured with resource triggering as the load-balancing behavior.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • hash-keys (Aggregated Multiservices) on page 32

secondary (Aggregated Packet Forwarding Engine)

Syntax	<code>secondary <i>anchoring-device-name</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> anchoring-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the secondary Flexible PIC Concentrator (FPC) for the anchor Packet Forwarding Engine redundancy. The Packet Forwarding Engine on the secondary FPC acts as the standby (backup) for the Packet Forwarding Engine on the primary FPCs and takes over as the active Packet Forwarding Engine when a Packet Forwarding Engine on a primary FPC fails.
Options	<i>anchoring-device-name</i> —Name of the FPC.
<div> NOTE: The interface must be a valid interface (<i>fpc-</i>) that is defined in the broadband gateway interface hierarchy.</div>	
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• anchoring-options (Aggregated Packet Forwarding Engine) on page 26• Configuring Interface Redundancy on page 15• Example: Configuring Broadband Gateway Redundancy on page 17

service-set (Aggregated Multiservices)

Syntax	<pre> service-set <i>service-set-name</i> { interface-service { load-balancing-options { hash-keys { egress-key (destination-ip source-ip); ingress-key (destination-ip source-ip); resource-triggered; } } service-interface <i>interface-name.unit-number</i>; } [tag-rule-sets <i>rule-set-name</i>]; [tag-rules <i>rule-name</i>]; service-set-options { subscriber-awareness; } } </pre>
Hierarchy Level	[edit services]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Support for aggregated multiservices (AMS) interfaces introduced in Junos OS Mobility Release 11.2W.</p>
Description	<p>Configure the service set with aggregated multiservices (AMS) for load balancing in service applications. Currently, Network Address Translation (NAT), stateful firewall, application-level gateway (ALG), HTTP header enrichment, and mobility are the service applications supported.</p> <p>The following ALGs are currently supported:</p> <ul style="list-style-type: none"> • FTP • Internet Control Message Protocol (ICMP) • Point-to-Point Tunneling Protocol (PPTP) • Real-Time Streaming Protocol (RTSP) • SQL *Net • TCP • traceroute • Trivial File Transfer Protocol (TFTP) • UDP <p>AMS for service applications (NAT, stateful firewall, and ALG) can be used for load balancing with or without high availability. Many-to-one (N:1) high availability (HA) is supported for service applications (NAT, stateful firewall, and ALG). In this case, one multiservices PIC is the backup for one or more (N) active multiservices PICs. If one of the active multiservices PICs goes down, then the backup replaces it as the active</p>

multiservices PIC. When the failed PIC comes back online, it becomes the new backup. This is called floating backup mode.



NOTE: In high availability for service applications, the configuration state is synchronized to the backup. However, the operational state of the active members is not synchronized to the backup. Therefore, in the case of failure, existing flows meant for the failed member are lost.

The following conditions are applicable if you use AMS for load balancing in service applications:

- All the member interfaces of the AMS interface must have the same packages configured for the respective service applications. For example, if **mams-5/0/0** is the active member and **mams-5/1/0** the backup, then both **mams-5/0/0** and **mams-5/1/0** must have the same packages.
 - For NAT, the member interfaces must have the **jservices-nat** package configured.
 - For stateful firewall, the member interfaces must have the **jservices-sfw** package configured.
 - For ALG, the member interfaces must have the **jservices-alg** package configured.
- The size of the object cache (**object-cache-size**) and the size of the policy database (**policy-db-size**) must be appropriately configured so that the memory requirements of the services application policy database are met.
- For anchor session PICs, currently, AMS member PICs operate only in 64-bit mode. Therefore the **boot-os embedded-junos64** configuration, at the **[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]** hierarchy level, is mandatory for all member interfaces.

The remaining statements are explained separately.

Options **service-set-name**—Name of the service set.

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

shared (IPsec)

Syntax	shared;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i> dial-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify that Dynamic End Point (DEP) IP Security (IPsec) tunnels are supported in shared logical interface (ifl) mode for the aggregated multiservices (AMS) interface. In shared ifl mode, one AMS ifl is shared by multiple DEP IPsec tunnels.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • dedicated (IPsec) on page 27 • dial-options (IPsec) on page 27

system (MobileNext Broadband Gateway Interfaces)

Syntax	<pre> system { pfes { [interface <i>interface-name</i>]; } service-pics { #P-GW only [interface <i>interface-name</i>]; } session-pics { [interface <i>interface-name</i>]; } } </pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify the different interfaces used to service the subscriber and for anchoring subscriber information in the broadband gateway. The remaining statements are explained separately.
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • [edit unified-edge gateways] Hierarchy Level • MobileNext Broadband Gateway Chassis Overview

unit (Aggregated Multiservices)

Syntax `unit interface-unit-number {
 dial-options {
 (dedicated | shared);
 ipsec-interface-id ipsec-interface-id;
 }
 family family;
 load-balancing-options {
 preferred-active interface-name;
 }
}`

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

The remaining statements are explained separately.

Options *interface-unit-number*—Number of the logical unit.



NOTE: Unit 0 is reserved and cannot be configured under the aggregated multiservices interface (ams).


Range: 1 through 16,384

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

Related Documentation

- [Configuring Session DPC Redundancy on page 13](#)
- [Example: Configuring Broadband Gateway Redundancy on page 17](#)
- [interfaces \(Aggregated Multiservices\) on page 41](#)

warm-standby (Aggregated Packet Forwarding Engine)

Syntax	warm-standby;
Hierarchy Level	[edit interfaces <i>interface-name</i> anchoring-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the anchor Packet Forwarding Engine redundancy in warm standby mode. In this mode, the secondary Flexible PIC Concentrator (FPC) takes over the role of the primary FPC when a Packet Forwarding Engine on the primary FPC fails. If a Packet Forwarding Engine fails on a primary FPC, then the entire FPC is switched to the secondary FPC.</p> <p>In warm-standby mode, the subscriber sessions are programmed only after the switchover from the primary FPC to the secondary FPC. Based on the subscriber traffic, the programming for some sessions is expedited if needed.</p> <div style="margin-top: 20px;">  <p>NOTE: When you configure warm standby mode, the switchover from the secondary FPC to the primary FPC takes place at the FPC level.</p> </div>
Default	The warm-standby mode is the default.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • anchoring-options (Aggregated Packet Forwarding Engine) on page 26 • Configuring Interface Redundancy on page 15 • Example: Configuring Broadband Gateway Redundancy on page 17

PART 3

Administration

- [Operational Commands on page 67](#)

CHAPTER 5

Operational Commands


request interface load-balancing revert (Aggregated Multiservices)

Syntax	<code>request interface load-balancing revert <i>interface-name</i></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Revert the aggregated multiservices member interface (mams-) from the inactive state to the active or backup state based on the configuration and the operational state of the aggregated multiservices interface.
Options	<i>interface-name</i> —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	view
Related Documentation	<ul style="list-style-type: none">• request interface load-balancing switchover (Aggregated Multiservices) on page 69
List of Sample Output	request interface load-balancing revert mams-4/0/0 (Aggregated Multiservices) on page 68
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

<code>request interface load-balancing revert mams-4/0/0 (Aggregated Multiservices)</code>	<code>user@host> request interface load-balancing revert mams-4/0/0 request succeeded</code>
--	---

request interface load-balancing switchover (Aggregated Multiservices)

Syntax	<code>request interface load-balancing switchover <i>interface-name</i> <force></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	<p>Switch the active member interface to the backup state.</p> <p>In the case of mobile control plane redundancy, the behavior depends on the replication state of the member interface:</p> <ul style="list-style-type: none"> • If the sync state is in-sync, then the active member is rebooted and the backup member becomes the new active member. • If the sync-state is in-progress, then the force option must be used to force the switchover. <div style="display: flex; align-items: center; margin-top: 10px;">  <div style="margin-left: 10px;"> <p>WARNING: In this case, there is a risk of losing subscriber information because the synchronization has not yet been completed.</p> </div> </div>
Options	<p><i>interface-name</i>—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.</p> <p>force—(Optional) Force the switchover from the active member to the backup member.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • request interface load-balancing revert (Aggregated Multiservices) on page 68
List of Sample Output	request interface load-balancing switchover force mams-4/0/0 (Aggregated Multiservices) on page 69
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```

request interface user@host> request interface load-balancing switchover force mams-4/0/0
load-balancing   Switchover Initiated
switchover force
mams-4/0/0
(Aggregated
Multiservices)

```

show services flows (Aggregated Multiservices)

Syntax `show services flows`
 `<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 Command introduced in Junos OS Release 9.5.
 Support for aggregated multiservices (AMS) introduced in Junos OS Mobility Release 11.2W.

Description Display the flow session table entries for the active members of the AMS interface for services applications.

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

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 total number of flows of the service sets in each member interface of the AMS.

destination-port *destination-port*—(Optional) Display information for the specified destination port. The range is from 0 through 65,535.

destination-prefix *destination-prefix*—(Optional) Display information for the specified destination prefix.

interface *interface-name*—(Optional) Display information about the specified interface. The **interface-name** is in the format **ms-fpc/pic/port**.

limit *number*—(Optional) Restrict the maximum number of entries displayed to the specified limit.

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**—Exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload protocol
- **gre**—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 the specified service set.

source-port *source-port*—(Optional) Display information for the specified source port. The range is from 0 through 65,535.

source-prefix *source-prefix*—(Optional) Display information for the specified source prefix.

Required Privilege Level	view
List of Sample Output	show services flows interface ams0 on page 72 show services flows count interface ams0 on page 73
Output Fields	Table 6 on page 72 lists the output fields for the show services flows (aggregated multiservices) command. Output fields are listed in the approximate order in which they appear.

Table 6: show services flows Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the aggregated multiservices member interface (mams-) and the aggregated multiservices interface (ams) to which it belongs.	All levels
Service set	Name of a service set. Individual empty service sets are not displayed. If no service set has any flows, a flow table header is displayed for each service set.	All levels
Flow Count	Number of flows in a session.	count only
Flow or Flow Prot	Protocol used for this flow.	All levels
Source	Source prefix of the flow in the format <i>source-prefix:port</i> . For ICMP flows, port information is not displayed.	All levels
Dest	Destination prefix of the flow. For ICMP flows, port information is not displayed.	All levels
State	Status of the flow: <ul style="list-style-type: none"> • 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. 	All levels
Dir	Direction of the flow: input (I) or output (O).	All levels
Frm count	Number of frames in the flow.	All levels
Byte count	Number of bytes in the flow.	extensive
Flow role	Flow role.	extensive
Timeout	Timeout value.	extensive
Flow path	Flow path: symmetric or asymmetric.	extensive

Sample Output

```

show services flows user@host> show services flows interface ams0
interface ams0      Interface: mams-1/0/0 (ams0), Service set: napt_set
Flow
UDP                 30.30.30.2:63    ->    40.40.40.2:63    Forward I      Frm count
UDP                 40.40.40.2:63    ->    30.30.30.160:6000 Forward O      83185
                                                           0

```

```
show services flows user@host> show services flows count interface ams0
count interface ams0
```

Interface	Service set	Flow count
mams-1/0/0	napt_set	38
mams-1/0/0	ssl	0
mams-1/1/0	napt_set	36
mams-1/1/0	ssl	0
mams-5/0/0	napt_set	18
mams-5/0/0	ssl	0
mams-5/1/0	napt_set	34
mams-5/1/0	ssl	0

show services nat mappings app

Syntax	show services nat mappings app <pool-name>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the Network Address Translation (NAT) mappings for paired IP address pooling (or address pooling paired [APP]) for the NAT pools on the multiservices interface.
Options	pool-name —(Optional) Display the NAT mappings for the NAT pool specified. (The NAT pools are configured at the [edit services nat] hierarchy level.)
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show services nat mappings eim on page 76 • show services nat mappings summary on page 78
List of Sample Output	show services nat mappings app on page 75
Output Fields	Table 7 on page 74 lists the output fields for the show services nat mappings app command. Output fields are listed in the approximate order in which they appear.

Table 7: show services nat mappings app Output Fields

Field Name	Field Description
Interface	Name of the multiservices interface (ms- or mams-).
Service set	Name of the service set for which the NAT mappings are displayed.
NAT pool	Name of the NAT pool.
Internal Address	Internal IP address that is being mapped.
External Address	External IP address to which the internal address is mapped.
Number of sessions	Number of sessions for which the NAT mapping has been done.
State	NAT mapping state. The following states are possible: <ul style="list-style-type: none"> • ACTIVE—Indicates that the entry is active and in use. • TIMEOUT—Indicates that the entry is not in use and will be deleted after the mapping-timeout, configured at the [edit services nat pool pool-name] hierarchy level, lapses.

Sample Output

```
show services nat mappings app  user@host> show services nat mappings app
                                Interface: ms-1/0/0, Service set: ss

                                NAT pool: p1
                                Internal Address  External Address  Number of sessions  State
                                10.10.10.3         30.30.30.3       1                   ACTIVE
                                10.10.10.2         30.30.30.2       2                   ACTIVE
```

show services nat mappings eim

Syntax	show services nat mappings eim <pool-name>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the Network Address Translation (NAT) mappings for Endpoint Independent Mapping (EIM) for the NAT pools on the multiservices interface.
Options	pool-name —(Optional) Display the NAT mappings for the NAT pool specified. (The NAT pools are configured at the [edit services nat] hierarchy level.)
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show services nat mappings app on page 74 • show services nat mappings summary on page 78
List of Sample Output	show services nat mappings eim on page 77
Output Fields	Table 8 on page 76 lists the output fields for the show services nat mappings eim command. Output fields are listed in the approximate order in which they appear.

Table 8: show services nat mappings eim Output Fields

Field Name	Field Description
Interface	Name of the multiservices interface (ms- or mams-).
Service set	Name of the service set for which the NAT mappings are displayed.
NAT pool	Name of the NAT pool.
Internal Address: Port	Internal IP address and the port that are being mapped.
External Address: Port	External IP address and the port to which the internal address and port are mapped.
Number of sessions	Number of sessions for which the NAT mapping has been done.
State	<p>NAT mapping state. The following states are possible:</p> <ul style="list-style-type: none"> • ACTIVE—Indicates that the entry is active and in use. • TIMEOUT—Indicates that the entry is not in use and will be deleted after the mapping-timeout, configured at the [edit services nat pool pool-name] hierarchy level, lapses.

Sample Output

```
show services nat mappings eim  user@host> show services nat mappings eim
                                Interface: ms-1/0/0, Service set: ss

                                NAT pool: p1
                                Internal Address    External Address    Number of sessions    State
                                10.10.10.3           30.30.30.3          1                      ACTIVE
                                10.10.10.2           30.30.30.2          2                      ACTIVE
```

show services nat mappings summary

Syntax	show services nat mappings summary
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the summary information about the Network Address Translation (NAT) mappings for the active multiservices interfaces.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show services nat mappings app on page 74 • show services nat mappings eim on page 76
List of Sample Output	show services nat mappings summary on page 78
Output Fields	Table 9 on page 78 lists the output fields for the show services nat mappings summary command. Output fields are listed in the approximate order in which they appear.

Table 9: show services nat mappings summary Output Fields

Field Name	Field Description
Interface	Name of the multiservices interface (ms- or mams-).
Total number of address mappings	Total number of address pooling paired (APP) mappings.
Total number of endpoint independent port mappings	Total number of endpoint-independent port mappings.

Sample Output

```

show services nat mappings summary  user@host> show services nat mappings summary
                                     Interface Name:                               ms-1/0/0
                                     Total number of address mappings:                1
                                     Total number of endpoint independent port mappings: 2

```

show services nat pool (Aggregated Multiservices)

Syntax	show services nat pool <brief detail> <pool-name>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display information about the Network Address Translation (NAT) pools and their current split among the active aggregated multiservices (AMS) member interfaces. In AMS NAT, the pool might be split among the active members based on the NAT type configured.
Options	<p>none—Display standard information about all the NAT pools for the ams interface.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>pool-name—(Optional) Display information about the specified NAT pool.</p>
Required Privilege Level	view
List of Sample Output	show services nat pool brief (Aggregated Multiservices) on page 80 show services nat pool detail (Aggregated Multiservices) on page 80 show services nat pool dynamic_pool detail on page 81
Output Fields	Table 10 on page 79 lists the output fields for the show services nat pool (aggregated multiservices) command. Output fields are listed in the approximate order in which they appear.

Table 10: show services nat pool Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the aggregated multiservices member interface (mams-) and the aggregated multiservices interface (ams) to which it belongs.	All levels
Service set	Name of the service set for the interface. Individual empty service sets are not displayed, but if none of the service sets has any flows, a flow table header is printed for each service set.	All levels
NAT pool	Name of the NAT pool for the interface.	All levels
Type or Translation type	Address translation type: basic-nat-pt , basic-nat44 , dnat-44 , dynamic-nat44 , NAPT-44 , or napt-pt .	All levels
Address or Address range	IPv4 address range of the pool.	All levels
Port or Port range	Port range of the pool. This is applicable only for dynamic NAT pools and is not displayed for static NAT pools.	All levels

Table 10: show services nat pool Output Fields (*continued*)

Field Name	Field Description	Level of Output
Ports used or Ports in use	Number of ports allocated in this pool with this name. This is applicable only for dynamic NAT pools and is not displayed for static NAT pools.	All levels
Out of port errors	Number of port allocation errors. This is applicable only for dynamic NAT pools and is not displayed for static NAT pools.	detail
Max ports used	Maximum number of ports used. This is applicable only for dynamic NAT pools and is not displayed for static NAT pools.	detail
Addresses in use	Number of addresses in use for dynamic source address NAT pools.	detail

Sample Output

```

user@host> show services nat pool brief
show services nat pool brief (Aggregated Multiservices)
Interface: mams-1/0/0 (ams0), Service set: napt_set
NAT pool      Type      Address                               Port      Ports used
napt_pool     NAPT-44  30.30.30.160-30.30.30.163           6000-8000 1
               30.30.30.176-30.30.30.176
Interface: mams-1/1/0 (ams0), Service set: napt_set
NAT pool      Type      Address                               Port      Ports used
napt_pool     NAPT-44  30.30.30.164-30.30.30.167           6000-8000 0
Interface: mams-5/0/0 (ams0), Service set: napt_set
NAT pool      Type      Address                               Port      Ports used
napt_pool     NAPT-44  30.30.30.168-30.30.30.171           6000-8000 0
Interface: mams-5/1/0 (ams0), Service set: napt_set
NAT pool      Type      Address                               Port      Ports used
napt_pool     NAPT-44  30.30.30.172-30.30.30.175           6000-8000 0

user@host> show services nat pool detail
show services nat pool detail (Aggregated Multiservices)
Interface: mams-1/0/0 (ams0), Service set: napt_set
NAT pool: napt_pool, Translation type: NAPT-44
Address range: 30.30.30.160-30.30.30.163
Address range: 30.30.30.176-30.30.30.176
Port range: 6000-8000, Ports in use: 19, Out of port errors: 0, Max ports
used: 19

Interface: mams-1/1/0 (ams0), Service set: napt_set
NAT pool: napt_pool, Translation type: NAPT-44
Address range: 30.30.30.164-30.30.30.167
Port range: 6000-8000, Ports in use: 18, Out of port errors: 0, Max ports
used: 18

Interface: mams-5/0/0 (ams0), Service set: napt_set
NAT pool: napt_pool, Translation type: NAPT-44
Address range: 30.30.30.168-30.30.30.171
Port range: 6000-8000, Ports in use: 9, Out of port errors: 0, Max ports used:
9

Interface: mams-5/1/0 (ams0), Service set: napt_set
NAT pool: napt_pool, Translation type: NAPT-44
Address range: 30.30.30.172-30.30.30.175
Port range: 6000-8000, Ports in use: 17, Out of port errors: 0, Max ports

```

used: 17

**show services nat pool
dynamic_pool detail**

```
user@host> show services nat pool dynamic_pool detail
Interface: mams-1/0/0 (ams0), Service set: napt_set
  NAT pool: napt_pool, Translation type: NAPT-44
    Address range: 30.30.30.160-30.30.30.163
    Address range: 30.30.30.176-30.30.30.176
    Port range: 6000-8000, Ports in use: 19, Out of port errors: 0, Max ports
used: 19

Interface: mams-1/1/0 (ams0), Service set: napt_set
  NAT pool: napt_pool, Translation type: NAPT-44
    Address range: 30.30.30.164-30.30.30.167
    Port range: 6000-8000, Ports in use: 18, Out of port errors: 0, Max ports
used: 18

Interface: mams-5/0/0 (ams0), Service set: napt_set
  NAT pool: napt_pool, Translation type: NAPT-44
    Address range: 30.30.30.168-30.30.30.171
    Port range: 6000-8000, Ports in use: 9, Out of port errors: 0, Max ports used:
9

Interface: mams-5/1/0 (ams0), Service set: napt_set
  NAT pool: napt_pool, Translation type: NAPT-44
    Address range: 30.30.30.172-30.30.30.175
    Port range: 6000-8000, Ports in use: 17, Out of port errors: 0, Max ports
used: 17
```

show services nat statistics

Syntax	show services nat statistics <interface <i>interface</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the NAT statistics for the multiservices interfaces present on the broadband gateway.
Options	interface <i>interface</i> —Name of the extension provider interface.
Required Privilege Level	view
List of Sample Output	show services nat statistics on page 87
Output Fields	Table 11 on page 82 lists the output fields for the show services nat statistics command. Output fields are listed in the approximate order in which they appear. Some of these fields are used internally by Juniper's engineers for troubleshooting.

Table 11: show services nat statistics Output Fields

Field Name	Field Description
Interface	Name of the multiservices interface.
Session Statistics	
Total Session Interest events	Total number of Session Interest events.
Total Session Create events	Total number of Session Create events.
Total Session Destroy events	Total number of Session Destroy events.
Total Session Pub Req events	Total number of Session Pub Req events.
Total Session Accepts	Total number of sessions accepted.
Total Session Discards	Total number of sessions discarded.
Total Session Ignores	Total number of sessions ignored.
Session interest thru pub event	Session interest through pub event.

Table 11: show services nat statistics Output Fields (*continued*)

Field Name	Field Description
ALG Session interest	Application-level gateway (ALG) session interest.
ALG Session Create	ALG Session Create
Packet Dst in NAT route	Sessions discarded due to packet destination in the NAT route.
Session Ext Alloc Failures	Session extension allocation failures.
Session Ext Set Failures	Session extension set failures.
Session Created for EIF	Number of sessions created for Endpoint Independent Filtering (EIF).
Session Created for EIM	Number of sessions created for Endpoint Independent Mapping (EIM).
NAT rule lookup failures	Number of NAT rule lookup failures.
NAT Allocation Statistics	
NAT allocation Successes	Number of successful NAT map allocations.
NAT allocation Failures	Number of NAT map allocation failures.
NAT Free Successes	NAT free successes.
NAT Free Failures	NAT free failures.
NAT EIM mapping reused	Number of NAT EIM mappings reused.
NAT EIM mapping allocation failures	Number of NAT EIM mapping allocation failures.
NAT EIM mapping Duplicate entry	Number of duplicate NAT EIM mappings.
NAT EIM mapping create failed	Number of failed NAT EIM mappings.
NAT EIM mapping Created	Number of NAT EIM mappings created.

Table 11: show services nat statistics Output Fields (*continued*)

Field Name	Field Description
NAT EIF mapping Free	Number of free NAT EIF mappings.
NAT EIM mapping Free	Number of free NAT EIM mappings.
NAT EIM waiting for init	Number of NAT EIM mappings waiting for initialization.
NAT EIM waiting for init failed	Number of NAT EIM mappings that failed initialization.
NAT EIM lookup and hold success	Number of successful NAT EIM lookups and holds.
NAT EIM lookup entry in timeout	NAT EIM lookup entry in timeout.
NAT EIM lookup timer cleared for timeout entry	NAT EIM lookup timer cleared for timeout entry.
NAT EIM lookup timeout entry without timer	NAT EIM lookup timeout entry without timer.
NAT EIM release without entry	NAT EIM release without entry.
NAT EIM release entry in timeout	NAT EIM release entry in timeout.
NAT EIM release race	NAT EIM release race.
NAT EIM release set entry for timeout	NAT EIM release set entry for timeout.
NAT EIM timer entry refreshed	NAT EIM timer entry refreshed.
NAT EIM timer invalid timer started	NAT EIM timer invalid timer started.
NAT EIM timer entry freed	NAT EIM timer entry freed.

Packet Statistics

Table 11: show services nat statistics Output Fields (*continued*)

Field Name	Field Description
Total Packets Processed	Total number of packets processed.
Total Packets Forwarded	Total number of packets forwarded.
Total Packets Discarded	Total number of packets discarded.
Total Packets Translated	Total number of packets translated.
Total Packets Restored	Total number of packets restored.
Translation Statistics	
Src IPv4 Translations	Number of source IPv4 translations.
Src IPv4 Restorations	Number of source IPv4 restorations.
Dst IPv4 Translations	Number of destination IPv4 translations.
Dst IPv4 Restorations	Number of destination IPv4 restorations.
Src Port Translations	Number of source port translations.
Src Port Restorations	Number of source port restorations.
Dst Port Translations	Number of destination port translations.
Dst Port Restorations	Number of destination port restorations.
ICMP ID Translations	Number of Internet Control Message Protocol (ICMP) translations.
ICMP ID Restorations	Number of ICMP restorations.
ICMP Error Translations	Number of ICMP error packets after translations.

Table 11: show services nat statistics Output Fields (*continued*)

Field Name	Field Description
TCP Port Translations	Number of TCP port translations.
TCP Port Restorations	Number of TCP port restorations.
UDP Port Translations	Number of UDP port translations.
UDP Port Restorations	Number of UDP port restorations.
GRE Call ID Translations	Number of generic routing encapsulation (GRE) call ID translations.
GRE Call ID Restorations	Number of GRE call ID restorations.
SRC IP restored in ICMP Error	Source IP restored in ICMP Error.
DST IP restored in ICMP Error	DST IP restored in ICMP Error.
SRC IP translated in ICMP Error	SRC IP translated in ICMP Error.
DST IP translated in ICMP Error	Destination IP translated in ICMP Error.
New SRC IP translated in ICMP Error	New source IP translated in ICMP Error.
Inner SRC IP restored in ICMP Error	Inner source IP restored in ICMP Error.
Inner SRC port restored in ICMP Error	Inner source port restored in ICMP Error.
Inner DST IP restored in ICMP Error	Inner destination IP restored in ICMP Error.
Inner SRC IP Translated in ICMP Error	Inner source IP translated in ICMP Error.

Table 11: show services nat statistics Output Fields (*continued*)

Field Name	Field Description
Inner SRC port Translated in ICMP Error	Inner source port translated in ICMP Error.
Inner DST IP Translated in ICMP Error	Inner destination IP translated in ICMP Error.
Misc Errors	
NAT error - no policy	Number of NAT errors of the no policy type.
NAT error - xlate free called with null ext	Number of NAT errors of the xlate free called with null ext type.
NAT error - ext free failed	Number of NAT errors of the ext free failed type.
NAT error - policy add failed	Number of NAT errors of the policy add failed type.
NAT error - policy delete failed	Number of NAT errors of the policy delete failed type.

Sample Output

```

show services nat statistics user@host> show services nat statistics
statistics                 Interface: ms-0/0/0

Session statistics
  Total Session Interest events      :12315
  Total Session Create events        :2
  Total Session Destroy events       :12315
  Total Session Pub Req events       :0
  Total Session Accepts               :12315
  Total Session Discards              :0
  Total Session Ignores               :0
  Session interest thru pub event     :0
  ALG Session interest               :0
  ALG Session Create                  :0
  Packet Dst in NAT route            :0
  Session Ext Alloc Failures          :0
  Session Ext Set Failures            :0
  Session Created for EIF             :1
  Session Created for EIM             :12314
  NAT rule lookup failures            :0

NAT Allocation statistics
  NAT allocation Successes            :12314
  NAT allocation Failures             :0
  NAT Free Successes                  :0

```

NAT Free Failures	:0
NAT EIM mapping reused	:12312
NAT EIM mapping allocation failures	:0
NAT EIM mapping Duplicate entry	:0
NAT EIM mapping create failed	:0
NAT EIM mapping Created	:2
NAT EIF mapping Free	:1
NAT EIM mapping Free	:12314
NAT EIM waiting for init	:0
NAT EIM waiting for init failed	:0
NAT EIM lookup and hold success	:12313
NAT EIM lookup entry in timeout	:0
NAT EIM lookup timer cleared for timeout entry	:0
NAT EIM lookup timeout entry without timer	:0
NAT EIM release without entry	:0
NAT EIM release entry in timeout	:0
NAT EIM release race	:0
NAT EIM release set entry for timeout	:2
NAT EIM timer entry refreshed	:0
NAT EIM timer invalid timer started	:2
NAT EIM timer entry freed	:2
Packet statistics	
Total Packets Processed	:2715735062
Total Packets Forwarded	:2715735062
Total Packets Discarded	:0
Total Packets Translated	:1818000836
Total Packets Restored	:897734226
Translation statistics	
Src IPv4 Translations	:400996
Src IPv4 Restorations	:897734226
Dst IPv4 Translations	:1817599840
Dst IPv4 Restorations	:0
Src Port Translations	:400996
Src Port Restorations	:897734226
Dst Port Translations	:1817599840
Dst Port Restorations	:0
ICMP ID Translations	:0
ICMP ID Restorations	:0
ICMP Error Translations	:0
TCP Port Translations	:0
TCP Port Restorations	:0
UDP Port Translations	:1818000836
UDP Port Restorations	:897734226
GRE CallID Translations	:0
GRE CallID Restorations	:0
SRC IP restored in ICMP Error	:0
DST IP restored in ICMP Error	:0
SRC IP translated in ICMP Error	:0
DST IP translated in ICMP Error	:0
New SRC IP translated in ICMP Error	:0
Inner SRC IP restored in ICMP Error	:0
Inner SRC port restored in ICMP Error	:0
Inner DST IP restored in ICMP Error	:0
Inner SRC IP Translated in ICMP Error	:0
Inner SRC port Translated in ICMP Error	:0
Inner DST IP Translated in ICMP Error	:0
Misc Errors	
NAT error - no policy	:0

```

NAT error - xlate free called with null ext      :0
NAT error - ext free failed                      :0
NAT error - policy add failed                   :0
NAT error - policy delete failed                :0

Interface: ms-1/1/0

Session statistics
  Total Session Interest events                  :6
  Total Session Create events                   :6
  Total Session Destroy events                  :7
  Total Session Pub Req events                  :0
  Total Session Accepts                        :6
  Total Session Discards                      :0
  Total Session Ignores                      :0
  Session interest thru pub event              :0
  ALG Session interest                        :0
  ALG Session Create                          :0
  Packet Dst in NAT route                     :0
  Session Ext Alloc Failures                   :0
  Session Ext Set Failures                     :0
  Session Created for EIF                      :0
  Session Created for EIM                     :6
  NAT rule lookup failures                     :0

NAT Allocation statistics
  NAT allocation Successes                     :6
  NAT allocation Failures                      :0
  NAT Free Successes                          :0
  NAT Free Failures                           :0
  NAT EIM mapping reused                       :3
  NAT EIM mapping allocation failures           :0
  NAT EIM mapping Duplicate entry              :0
  NAT EIM mapping create failed                :0
  NAT EIM mapping Created                     :3
  NAT EIF mapping Free                         :0
  NAT EIM mapping Free                         :7
  NAT EIM waiting for init                     :0
  NAT EIM waiting for init failed              :0
  NAT EIM lookup and hold success              :2
  NAT EIM lookup entry in timeout              :1
  NAT EIM lookup timer cleared for timeout entry :1
  NAT EIM lookup timeout entry without timer   :0
  NAT EIM release without entry                :0
  NAT EIM release entry in timeout             :0
  NAT EIM release race                        :0
  NAT EIM release set entry for timeout        :5
  NAT EIM timer entry refreshed                :0
  NAT EIM timer invalid timer started          :4
  NAT EIM timer entry freed                    :4

Packet statistics
  Total Packets Processed                      :2733886586
  Total Packets Forwarded                      :2733886586
  Total Packets Discarded                      :0
  Total Packets Translated                     :1836152360
  Total Packets Restored                       :897734226

Translation statistics
  Src IPv4 Translations                       :1836152360
  Src IPv4 Restorations                       :0

```

Dst IPv4	Translations	:0
Dst IPv4	Restorations	:897734226
Src Port	Translations	:1836152360
Src Port	Restorations	:0
Dst Port	Translations	:0
Dst Port	Restorations	:897734226
ICMP ID	Translations	:0
ICMP ID	Restorations	:0
ICMP Error	Translations	:0
TCP Port	Translations	:0
TCP Port	Restorations	:0
UDP Port	Translations	:1836152360
UDP Port	Restorations	:897734226
GRE CallID	Translations	:0
GRE CallID	Restorations	:0
SRC IP	restored in ICMP Error	:0
DST IP	restored in ICMP Error	:0
SRC IP	translated in ICMP Error	:0
DST IP	translated in ICMP Error	:0
New SRC IP	translated in ICMP Error	:0
Inner SRC IP	restored in ICMP Error	:0
Inner SRC port	restored in ICMP Error	:0
Inner DST IP	restored in ICMP Error	:0
Inner SRC IP	Translated in ICMP Error	:0
Inner SRC port	Translated in ICMP Error	:0
Inner DST IP	Translated in ICMP Error	:0
Misc Errors		
NAT error - no policy		:0
NAT error - xlate free called with null ext		:0
NAT error - ext free failed		:0
NAT error - policy add failed		:0
NAT error - policy delete failed		:0

show services service-sets summary

Syntax	show services service-sets summary <interface <i>interface</i>>
Release Information	Command introduced before Junos OS Release 7.4. Display of the CPU usage in the output introduced in Junos OS Mobility Release 11.2W.
Description	Display the summary information about the service sets for multiservices (MS) interfaces.
Options	interface <i>interface</i> —Name of the adaptive services interface (ms-).
Required Privilege Level	view
List of Sample Output	show services service-sets summary on page 91
Output Fields	Table 12 on page 91 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 12: show services service-sets summary Output Fields

Field Name	Field Description
Interface	Name of the multiservices member interface (ms-).
Service sets configured	Total number of service sets configured on the interface.
Bytes used	Total number of bytes used by stateful services for runtime information. (The object-cache-size statement is used to set the memory allocated for runtime services.) The following information is also displayed: <ul style="list-style-type: none"> Memory Alarm (zone): If the amount of free memory goes below the limit (64 MB for 32-bit Junos OS and 128 MB for 64-bit Junos OS), an overload alert (OVLD) is displayed. If not, then nothing is displayed. Percentage of the total number of bytes used.
Policy bytes used	Total number of policy bytes used and the percentage used. Policy bytes is the amount of memory used for user configuration and correlates with the policy-db-size statement.
CPU Utilization	Percentage of CPU utilization per PIC. The following information is also displayed: <ul style="list-style-type: none"> CPU Alarm (Zone): If the CPU utilization goes above the configured limit, then an overload alert (OVLD) is displayed. If not, then nothing is displayed.

Sample Output

```

show services user@host> show services service-sets summary
service-sets summary
Service sets
CPU
Interface    configured      Bytes used    Policy bytes used    utilization

```

ms-0/0/0	1	385021900	(81.96%)	299796 (0.44%)	92.89 % OVLD
----------	---	-----------	----------	-----------------	--------------

show services sessions (Aggregated Multiservices)

Syntax	<pre>show services sessions <brief extensive terse> <application-protocol <i>protocol</i>> <count> <destination-port <i>destination-port</i>> <destination-prefix <i>destination-prefix</i>> <interface <i>interface-name</i>> <limit <i>number</i>> <protocol <i>protocol</i>> <service-set <i>service-set</i>> <source-port <i>source-port</i>> <source-prefix <i>source-prefix</i>></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 10.4.</p> <p>Support for aggregated multiservices (AMS) introduced in Junos OS Mobility Release 11.2W.</p>
Description	Display the session information for each service set in each member interface of the AMS interface.
Options	<p>none—Display standard information about all sessions.</p> <p>brief extensive terse—(Optional) Display the specified level of output.</p> <p>application-protocol—(Optional) Display information about one of the following application protocols:</p> <ul style="list-style-type: none"> • 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 <p>count—(Optional) Display a count of the matching entries.</p> <p>destination-port <i>destination-port</i>—(Optional) Display information for a particular destination port. The range of values is from 0 through 65,535.</p> <p>destination-prefix <i>destination-prefix</i>—(Optional) Display information for a particular destination prefix.</p>

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

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

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

- **number**—Numeric protocol value from 0 through 255
- **ah**—IPsec Authentication Header protocol
- **egp**—An exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload protocol
- **gre**—A generic routing encapsulation protocol
- **icmp**—Internet Control Message Protocol
- **icmp6**—Internet Control Message Protocol version 6
- **igmp**—Internet Group Management Protocol
- **ipip**—IP-over-IP encapsulation protocol
- **ospf**—Open Shortest Path First protocol
- **pim**—Protocol Independent Multicast protocol
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

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

source-port *source-port*—(Optional) Display information for a particular source port. The range of values is from 0 through 65,535.

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

Required Privilege Level	view
List of Sample Output	show services sessions brief on page 95 show services sessions interface mams-5/0/0 extensive on page 96 show services sessions terse on page 98 show services sessions count on page 99
Output Fields	Table 13 on page 95 lists the output fields for the show services sessions command. Output fields are listed in the approximate order in which they appear.

Table 13: 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: <ul style="list-style-type: none"> • 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.
State	Status of the flow: <ul style="list-style-type: none"> • 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 user@host> show services sessions brief
brief
```

show services sessions
interface mams-5/0/0
extensive

```
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 0      0
```

```
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 0      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 0      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 0      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 0      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 Pugin 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 0 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 Pugin 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 0 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 Pugin 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 0 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 Pugin 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 0 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 user@router> show services sessions terse
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 0        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 0        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 0        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  ssl          0
mams-1/1/0  napt_set     18
mams-1/1/0  ssl          0
mams-5/0/0  napt_set     9
mams-5/0/0  ssl          0
mams-5/1/0  napt_set     17
mams-5/1/0  ssl          0

```

show interfaces anchor-group (Aggregated Packet Forwarding Engine)

Syntax `show interfaces anchor-group`
`<brief | detail>`
`interface-name`

Release Information Command introduced in Junos OS Mobility Release 11.2W.

Description Display interface information for the aggregated Packet Forwarding Engine group.

Options **none**—(Same as brief) Display a summary of the aggregated Packet Forwarding Engine interface information.

brief | detail—(Optional) Display the specified level of output.

interface-name—Name of the interface within the anchor Packet Forwarding Engine group.



NOTE: The interface must be an aggregated Packet Forwarding Engine interface (apfe-).

Required Privilege Level view

Related Documentation • [show unified-edge ggsn-pgw system interfaces on page 110](#)

List of Sample Output [show interfaces anchor-group brief on page 101](#)
[show interfaces anchor-group detail on page 102](#)

Output Fields [Table 14 on page 100](#) lists the output fields for the `show interfaces anchor-group` command. Output fields are listed in the approximate order in which they appear.

Table 14: show interfaces anchor-group

Field Name	Field Description	Level of Output
Redundancy Status Legend	<p>Legend for the redundancy status.</p> <ul style="list-style-type: none"> • Active—Indicates that the anchor Packet Forwarding Engine is operational. • Inactive—Indicates that the anchor Packet Forwarding Engine is not operational. • PF—Indicates that the primary Packet Forwarding Engine anchor has failed. • WS—Indicates that the primary Packet Forwarding Engine is protected by a secondary Packet Forwarding Engine in warm standby mode. 	All levels
Group	Name of the aggregated Packet Forwarding Engine group.	brief none
Mode	Redundancy mode in which the aggregated Packet Forwarding Engine group operates. Currently, only warm standby mode is supported.	brief none

Table 14: show interfaces anchor-group (*continued*)

Field Name	Field Description	Level of Output
Sub-group ID	Redundancy subgroups within the anchor Packet Forwarding Engine group configuration that has FPCs as members. This is derived out of the Packet Forwarding Engines on a given FPC. For example, if the first Packet Forwarding Engine is assigned the number 0, then all the other Packet Forwarding Engines with sub-group ID 0 form the N:1 redundancy group.	brief none
Interface	Anchor Packet Forwarding Engine interface (pfe-).	brief detail none
Configured State	State in which the anchor Packet Forwarding Engine was configured. <ul style="list-style-type: none"> • Primary: Indicates that the anchor Packet Forwarding Engine is in the pool of primary members. • Secondary: Indicates that the anchor Packet Forwarding Engine is a backup to all the primary members. 	brief detail none
Operational State	Indicates whether the anchor Packet Forwarding Engine is operational (Active) or not operational (Inactive).	brief detail none
Redundancy State	Redundancy state (primary or secondary) in which the anchor Packet Forwarding Engine was configured.	brief detail none
Group Name	Name of the aggregated Packet Forwarding Engine group.	detail
Group Mode	Redundancy mode in which the aggregated Packet Forwarding Engine group operates. Currently, only warm standby mode is supported.	detail
Group Id	Internal ID generated for the group.	detail
Switchover information	Switchover details, if any.	detail
Subgroup identifier	Redundancy subgroups within the anchor Packet Forwarding Engine group configuration that has FPCs as members. This is derived out of the Packet Forwarding Engines on a given FPC. For example, if the first Packet Forwarding Engine is assigned the number 0, then all the other Packet Forwarding Engines with subgroup ID 0 form the N:1 redundancy group.	detail

Sample Output

```

show interfaces anchor-group brief
user@host> show interfaces anchor-group brief
Redundancy Status Legend:

Active: Operational      Inactive: Non-operational
MS: Manually switched    PF: Primary failed
HS: Hot standby          WS: Warm standby

Group   Mode   Sub-group   Interface   Configured   Operational   Redundancy
      ID                               State        State        State
-----
apfe0   WS     0           pfe-4/0/0   Primary     Active        Primary
          pfe-5/0/0   Secondary    Active        Secondary

```

2	pfe-4/2/0	Primary	Active	Primary
	pfe-5/2/0	Secondary	Active	Secondary

show interfaces
anchor-group detail

```
user@host> show interfaces anchor-group detail
Active: Operational          Inactive: Non-operational
MS: Manually switched       PF: Primary failed
HS: Hot standby             WS: Warm standby

Group Name: apfe0
Group Mode: WS              Group Id: 65
Switchover information: None
Interface pfe-4/2/0
  Configured state: Primary  Operational state: Active
  Redundancy state: Primary
  Subgroup identifier: 2
Interface pfe-4/0/0
  Configured state: Primary  Operational state: Active
  Redundancy state: Primary
  Subgroup identifier: 0
Interface pfe-5/0/0
  Configured state: Secondary Operational state: Active
  Redundancy state: Secondary
  Subgroup identifier: 0
Interface pfe-5/2/0
  Configured state: Secondary Operational state: Active
  Redundancy state: Secondary
  Subgroup identifier: 2
```

show interfaces load-balancing (Aggregated Multiservices)

Syntax	show interfaces load-balancing <detail> <interface-name>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display information about the aggregated multiservices interface (ams) as well as its individual member interfaces and the status of the replication state.
Options	<p>none—Display a summary of the aggregated multiservices interface information.</p> <p>detail—(Optional) Display the specified level of output.</p> <p>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.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw system interfaces on page 110
List of Sample Output	show interfaces load-balancing on page 104 show interfaces load-balancing detail on page 104 show interfaces load-balancing ams0 detail on page 105
Output Fields	Table 15 on page 103 lists the output fields for the show interfaces load-balancing command. Output fields are listed in the approximate order in which they appear.

Table 15: show interfaces load-balancing Output Fields

Field Name	Field Description	Level of Output
Interface	Aggregated multiservices interface (ams).	detail none
State	<p>State of the aggregated multiservices interface. The following states are possible:</p> <ul style="list-style-type: none"> • Wait for Members—None of the member interfaces are powered on yet. • Members Seen—All of the member interfaces are online. • Wait Timer—At least one of the member interfaces has joined the ams interface. • Up—The ams interface is up with the current joined member interfaces. 	detail none
Last change	Time (in <i>hh:mm:ss [hours:minutes:seconds]</i> format) when the state last changed.	detail none
Members	Number of member interfaces (mams-).	none

Table 15: show interfaces load-balancing Output Fields (*continued*)

Field Name	Field Description	Level of Output
Member count	Number of member interfaces (mams-).	detail
HA Model	High availability (HA) model supported on the interface.	detail none
Members	<p>The following information about the member interfaces is displayed:</p> <ul style="list-style-type: none"> • Interface—Name of the member interface. • Weight—This output can be ignored for the current release. • State—Indicates the state of the member interface (mams-). The following states are possible: <ul style="list-style-type: none"> • Active—The member is an active member. • Backup—The member is a backup. • Discard—The member has not yet rejoined the ams interface after failure. • Down—The member has not yet powered on. • Inactive—The member has failed to rejoin the ams interface within the configured rejoin-timeout. • Invalid—The Multiservices PIC corresponding to the member interface has been configured but is not physically present in the chassis. 	detail
Sync-state	<p>Synchronization (sync) status of the control plane redundancy. The sync state is displayed only when the ams interface is Up.</p> <ul style="list-style-type: none"> • Interface—Name of the member interface. • Status—The synchronization status of the member interfaces. <ul style="list-style-type: none"> • 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 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 user@host> show interfaces load-balancing
load-balancing Interface State      Last change  Members  HA Model
                  ams0      Up           00:10:02    4        Many-to-One

```

```

show interfaces user@host> show interfaces load-balancing detail
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 ams0 detail
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 ipsec-vpn ipsec security-associations

Syntax	show services ipsec-vpn ipsec security-associations <brief detail extensive> <service-set service-set-name>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(Adaptive services interface only) Display IPsec security associations for the specified service set. If no service set is specified, the security associations for all service sets are displayed.
Options	<p>none—Display standard information about IPsec security associations for all service sets.</p> <p>brief detail extensive—(Optional) Display the specified level of output.</p> <p>service-set service-set-name—(Optional) Display information about a particular service set.</p>
Required Privilege Level	view
List of Sample Output	show services ipsec-vpn ipsec security associations detail on page 108 show services ipsec-vpn ipsec security associations extensive on page 108
Output Fields	Table 16 on page 106 lists the output fields for the show services ipsec-vpn ipsec security-associations command. Output fields are listed in the approximate order in which they appear.

Table 16: show services ipsec-vpn ipsec security-associations Output Fields

Field Name	Field Description	Level of Output
Service set	Name of the service set for which the IPsec security associations are defined. If appropriate, includes the outside service interface VRF name.	All levels
Rule	Name of the rule set applied to the security association.	detail extensive
Term	Name of the IPsec term applied to the security association.	detail extensive
Tunnel index	Numeric identifier of the specific IPsec tunnel for the security association.	detail extensive
Anchored PIC	Services PIC on which the IPsec tunnel is anchored. This field is displayed only if the service set is applied over an AMS interface; for example ams0 .	detail extensive
Local gateway	Gateway address of the local system.	All levels
Remote gateway	Gateway address of the remote system.	All levels
IPsec inside interface	Name of the logical interface hosting the IPsec tunnels.	All levels

Table 16: show services ipsec-vpn ipsec security-associations Output Fields (*continued*)

Field Name	Field Description	Level of Output
Local identity	Prefix and port number of the local end.	All levels
Remote identity	Prefix and port number of the remote end.	All levels
Primary remote gateway	IP address of the configured primary remote peer.	All levels
Backup remote gateway	IP address of the configured backup remote peer.	All levels
State	State of the primary or backup interface: Active , Offline , or Standby . Both ES PICs are initialized to Offline . For primary and backup peers, State can be Active or Standby . If both peers are in a state of Standby , no connection exists yet between the two peers.	All levels
Failover counter	Number of times a PIC switched between the primary and backup interfaces, or the number of times the tunnel switched between the primary and remote peers since the software was activated.	All levels
Direction	Direction of the security association: inbound or outbound .	All levels
SPI	Value of the security parameter index.	All levels
AUX-SPI	Value of the auxiliary security parameter index: <ul style="list-style-type: none"> When the value of Protocol is AH or ESP, AUX-SPI is always 0. When the value of Protocol is AH+ESP, AUX-SPI is always a positive integer. 	All levels
Mode	Mode of the security association: <ul style="list-style-type: none"> transport—Protects single host-to-host protections. tunnel—Protects connections between security gateways. 	detail extensive
Type	Type of security association: <ul style="list-style-type: none"> manual—Security parameters require no negotiation. They are static, and are configured by the user. dynamic—Security parameters are negotiated by the IKE protocol. Dynamic security associations are not supported in transport mode. 	detail extensive
State	Status of the security association: <ul style="list-style-type: none"> Installed—The security association is installed in the security association database. (For transport mode security associations, the value of State must always be Installed.) Not installed—The security association is not installed in the security association database. 	detail extensive

Table 16: show services ipsec-vpn ipsec security-associations Output Fields (*continued*)

Field Name	Field Description	Level of Output
Protocol	Protocol supported: <ul style="list-style-type: none"> transport mode supports Encapsulation Security Protocol (ESP) or Authentication Header (AH). tunnel mode supports ESP or AH+ESP. 	All levels
Authentication	Type of authentication used: hmac-md5-96 , hmac-sha1-96 , or none .	detail extensive
Encryption	Type of encryption algorithm used: aes-cbc (128 bits) , aes-cbc (192 bits) , aes-cbc (256 bits) , des-cbc , 3des-cbc , or None .	detail
Soft lifetime Hard lifetime	Each lifetime of a security association (SA) has two display options, hard and soft, one of which must be present for a dynamic security association. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPsec key management system that the SA is about to expire. This information allows the key management system to negotiate a new SA before the hard lifetime expires. <ul style="list-style-type: none"> Expires in seconds seconds—Number of seconds left until the security association expires. Expires in kilobytes kilobytes—Number of kilobytes left until the security association expires. 	detail extensive
Anti-replay service	State of the service that prevents packets from being replayed: Enabled or Disabled .	detail extensive
Replay window size	Configured size, in packets, of the antireplay service window: 32 or 64 . The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets. If the replay window size is 0 , antireplay service is disabled.	detail

Sample Output

```

show services ipsec-vpn ipsec security associations detail
user@host> show services ipsec-vpn ipsec security-associations detail
Service set: huffer, IKE Routing-instance: default

Rule: _junos_, Term: tunnel1, Tunnel index: 1, Anchored pic: mams-5/1/0
Local gateway: 4.1.1.2, Remote gateway: 4.1.1.1
IPSec inside interface: ams0.1, Tunnel MTU: 1500
Local identity: ipv4(any:0,[0..3]=4.1.1.2)
Remote identity: ipv4(any:0,[0..3]=4.1.1.1)

show services ipsec-vpn ipsec security associations extensive
user@host> show services ipsec-vpn ipsec security-associations extensive
Service set: snart, IKE Routing-instance: default

Rule: _junos_, Term: tunnel1, Tunnel index: 1, Anchored pic: mams-5/1/0
Local gateway: 3.1.100.101, Remote gateway: 3.1.100.2
IPSec inside interface: ams0.1, Tunnel MTU: 1500
Local identity: ipv4(any:0,[0..3]=5.1.0.2)
Remote identity: ipv4(any:0,[0..3]=4.1.0.2)

```


Direction: inbound, SPI: 2417504417, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 28704 seconds
Hard lifetime: Expires in 28794 seconds
Anti-replay service: Enabled, Replay window size: 128

Direction: outbound, SPI: 4201112312, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 28704 seconds
Hard lifetime: Expires in 28794 seconds
Anti-replay service: Enabled, Replay window size: 128

show unified-edge ggsn-pgw system interfaces

Syntax	show unified-edge ggsn-pgw system interfaces <gateway gateway>
Release Information	Command introduced in Junos OS Mobility Release 11.2W. gateway option introduced in Junos OS Mobility Release 11.4W.
Description	Display information about the aggregated Packet Forwarding Engine and the aggregated multiservices (AMS) interfaces and their states on one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then information for all GGSNs and P-GWs is displayed.
Options	none —Display information for one or more GGSNs and P-GWs. gateway gateway-name —(Optional) Display information for the specified gateway.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show interfaces anchor-group (Aggregated Packet Forwarding Engine) on page 100 • show interfaces load-balancing (Aggregated Multiservices) on page 103 • show unified-edge ggsn-pgw resource-manager clients • show unified-edge ggsn-pgw system interfaces service-mode
List of Sample Output	show unified-edge ggsn-pgw system interfaces on page 111
Output Fields	Table 17 on page 110 lists the output fields for the show unified-edge ggsn-pgw system interfaces command. Output fields are listed in the approximate order in which they appear.

Table 17: show unified-edge ggsn-pgw system interfaces

Field Name	Field Description
Gateway	Name of the GGSN or P-GW.
Interfaces	Name of the interface: <ul style="list-style-type: none"> • Aggregated multiservices; for example, ams0 • Aggregated Packet Forwarding Engine; for example, apfe1 • Member of aggregated multiservices; for example, mams-1/0/0 • Multiservices; for example, ms-1/0/0 • Packet Forwarding Engine; for example, pfe-0/1/0
Members	For ams and apfe interfaces, the member interfaces that are part of the aggregated interfaces are displayed.
Operational State	Indicates whether the interface is operational (Active) or not (Inactive).

Table 17: show unified-edge ggsn-pgw system interfaces (*continued*)

Field Name	Field Description
Redundancy Role	Redundancy state in which the interface is configured: <ul style="list-style-type: none"> • Primary—The interface is a primary member. • Secondary—The interface is a backup to all the primary members. • Standalone—The interface has not been configured for redundancy.

Sample Output

```

show unified-edge ggsn-pgw system interfaces
user@host> show unified-edge ggsn-pgw system interfaces
Gateway: PGW
      Interfaces      Members      Operational      Redundancy
                  State
ms-1/0/0             Active        Standalone
ms-1/1/0             Active        Standalone
ms-2/0/0             Active        Standalone
ms-2/1/0             Active        Standalone
pfe-0/0/0            Active        Standalone
pfe-0/1/0            Active        Standalone
pfe-0/2/0            Active        Standalone
pfe-0/3/0            Active        Standalone

```

show unified-edge sgw system interfaces

Syntax	show unified-edge sgw system interfaces <gateway gateway>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display information about the aggregated Packet Forwarding Engine and the aggregated multiservices (AMS) interfaces and their states on one or more configured Serving Gateways (S-GWs). If a gateway is not specified, then information for all configured S-GWs is displayed.
Options	gateway gateway —(Optional) Display interface information for the specified gateway.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show interfaces anchor-group (Aggregated Packet Forwarding Engine) on page 100 • show interfaces load-balancing (Aggregated Multiservices) on page 103 • show unified-edge sgw resource-manager clients • show unified-edge sgw system interfaces service-mode
List of Sample Output	show unified-edge sgw system interfaces on page 113
Output Fields	Table 18 on page 112 lists the output fields for the show unified-edge sgw system interfaces command. Output fields are listed in the approximate order in which they appear.

Table 18: show unified-edge sgw system interfaces Output Fields

Field Name	Field Description
Gateway	Name of the S-GW.
Interfaces	Name of the interface: <ul style="list-style-type: none"> • Aggregated multiservices; for example, ams0 • Aggregated Packet Forwarding Engine, for example, apfe1 • Member of aggregated multiservices; for example mams-1/0/0 • Multiservices; for example, ms-3/0/0 • Packet Forwarding Engine; for example pfe-4/2/0
Members	For ams and apfe interfaces, the member interfaces that are part of the aggregated interfaces are displayed.
Operational State	Indicates whether the interface is operational (Active) or not (Inactive).

Table 18: show unified-edge sgw system interfaces Output Fields (*continued*)

Field Name	Field Description
Redundancy Role	<p>Redundancy state in which the interface is configured:</p> <ul style="list-style-type: none"> • Primary—The interface is a primary member. • Secondary—The interface is a backup to all the primary members. • Standalone—The interface is not configured for redundancy.

Sample Output

```

show unified-edge sgw system interfaces user@host> show unified-edge sgw system interfaces
Gateway: SGW
  Interfaces      Members      Operational State      Redundancy Role
ms-3/0/0          Active       Standalone
ms-3/1/0          Inactive    Standalone
pfe-4/0/0         Active       Standalone
pfe-4/2/0         Active       Standalone

```


PART 4

Index

- [Index on page 117](#)

Index

Symbols

#, comments in configuration statements.....	xi
(), in syntax descriptions.....	xi
< >, in syntax descriptions.....	x
[], in configuration statements.....	xi
{ }, in configuration statements.....	xi
(pipe), in syntax descriptions.....	xi

A

anchoring-options statement.....	26
anchors	
broadband gateway.....	7
apfe-group-set statement.....	25

B

braces, in configuration statements.....	xi
brackets	
angle, in syntax descriptions.....	x
square, in configuration statements.....	xi
broadband gateway	
anchors.....	7
interface redundancy.....	6
interfaces redundancy configuration	
example.....	17
redundancy configuration.....	4
redundancy configuration example.....	17
Routing Engine redundancy.....	4
session DPC redundancy.....	5
session DPC redundancy configuration	
example.....	17

C

chassis	
redundancy configuration.....	13, 15
comments, in configuration statements.....	xi
configuration	
broadband gateway interface PFEs.....	4
broadband gateway services PICs.....	4
configuration example	
redundancy.....	17

configuring chassis	
interfaces for mobility redundancy.....	15
session DPC redundancy.....	13
configuring interfaces for mobility	
redundancy.....	15
configuring redundancy	
interfaces for mobility.....	15
session DPC.....	13
configuring session DPC	
redundancy.....	13
conventions	
text and syntax.....	x
curly braces, in configuration statements.....	xi
customer support.....	xi
contacting JTAC.....	xi

D

dedicated statement	
IPsec.....	27
dial-options statement	
IPsec.....	27
documentation	
comments on.....	xi
drop-member-traffic statement	
aggregated multiservices.....	28

E

edit interfaces ams statement hierarchy.....	21
edit interfaces apfe statement hierarchy.....	22
egress-key statement	
aggregated multiservices.....	29
enable-rejoin statement	
aggregated multiservices.....	30

F

failover	
broadband gateway anchors.....	7
family statement	
aggregated multiservices.....	31
font conventions.....	x

H

hash-keys statement	
aggregated multiservices.....	32
high-availability-options statement	
aggregated multiservices.....	34

I

ingress-key statement	
aggregated multiservices.....	35
interface redundancy configuration example	
broadband gateway.....	17
interface statement	
Packet Forwarding Engine.....	36
services PIC.....	38
session PIC.....	39
interface-service statement	
aggregated multiservices.....	40
interfaces for mobility	
redundancy configuration.....	15
interfaces statement	
aggregated multiservices.....	41
aggregated Packet Forwarding Engine.....	43
IPsec services	
adaptive services interfaces	
IPSec security associations,	
displaying.....	106
ipsec-interface-id statement	
IPsec.....	44

L

load-balancing-options statement	
aggregated multiservices.....	45, 46
IPsec.....	47

M

manuals	
comments on.....	xi
many-to-one statement	
aggregated multiservices.....	48
member-failure-options statement	
aggregated multiservices.....	49
member-interface statement	
aggregated multiservices.....	52

O

overview	
interface redundancy.....	6
Routing Engine redundancy.....	4
session DPC redundancy.....	5

P

parentheses, in syntax descriptions.....	xi
pfes statement.....	23
preferred-active statement	
IPsec.....	53

primary-list statement.....	54
-----------------------------	----

R

redistribute-all-traffic statement	
aggregated multiservices.....	55
redundancy	
anchor failover.....	7
broadband gateway.....	4, 5, 6
configuration example.....	17
configuring session DPC.....	13, 15
redundancy configuration example	
broadband gateway.....	17
rejoin-timeout statement	
aggregated multiservices.....	56
request interface load-balancing revert (aggregated multiservices) command.....	68
request interface load-balancing switchover (aggregated multiservices) command.....	69
resource-triggered statement	
aggregated multiservices.....	57

S

secondary statement	
aggregated Packet Forwarding Engine.....	58
service-pics statement.....	23
service-set statement	
aggregated multiservices.....	59
session DPC	
redundancy configuration.....	13
session DPC redundancy configuration example	
broadband gateway.....	17
session-pics statement.....	24
shared statement	
IPsec.....	61
show interfaces anchor-group command	
aggregated Packet Forwarding Engine.....	100
show interfaces load-balancing command	
aggregated multiservices.....	103
show services flows command	
aggregated multiservices.....	70
show services ipsec-vpn ipsec security-associations command.....	106
show services nat mappings app command.....	74
show services nat mappings eim command.....	76
show services nat mappings summary	
command.....	78
show services nat pool command	
aggregated multiservices.....	79
show services nat statistics command.....	82

show services service-sets summary command.....	91
show services sessions command	
aggregated multiservices.....	93
show unified-edge ggsn-pgw system interfaces	
command.....	110
show unified-edge sgw system interfaces	
command.....	112
support, technical See technical support	
syntax conventions.....	x
system statement.....	61

T

technical support	
contacting JTAC.....	xi

U

unit statement	
aggregated multiservices.....	62

W

warm-standby statement	
aggregated Packet Forwarding Engine.....	63

