JUNIPER NETWORKS | Engineering Simplicity

Junos Multi-Access User Plane User Guide

Published
2020-09-23

JUNOS

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

Junos Multi-Access User Plane User Guide

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About the Documentation

IN THIS SECTION

Use this guide to understand the Junos Multi-Access User Plane and how to configure an MX Series router as an SAEGW-U to provide high-throughput data processing for your SAEGW-C.

Documentation and Release Notes

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

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

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

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
       scripts {
           commit {
               file ex-script.xsl;
           }
       }
   }
   interfaces {
       fxp0 {
           disable;
           unit 0 {
               family inet {
                   address 10.0.0.1/24;
               }
           }
       }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   user@host# edit system scripts
   [edit system scripts]
   ```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

   ```
   [edit system scripts]
   user@host# load merge relative /var/tmp/ex-script-snippet.conf
   load complete
   ```

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

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

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

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

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

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

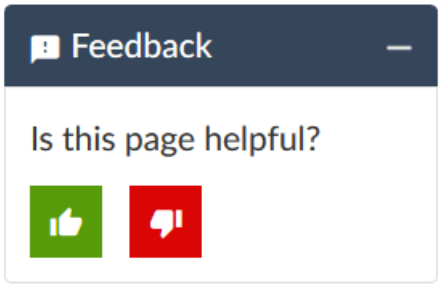
Table 2: Text and Syntax Conventions *(continued)*

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

Documentation Feedback

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

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



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

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

Self-Help Online Tools and Resources

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

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

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

Creating a Service Request with JTAC

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

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

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

CHAPTER 1

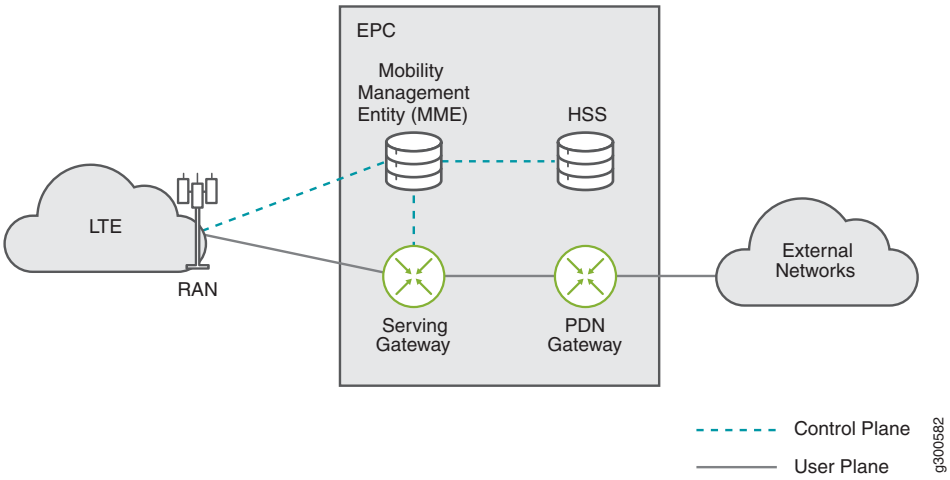
Understanding the Junos Multi-Access User Plane

Junos Multi-Access User Plane Overview

The 3GPP Release 8 introduced the Evolved Packet Core (EPC) for core network architecture. As Figure 1 on page 13 shows, the four main EPC network elements are:

- Serving Gateway
- Packet Data Network (PDN) Gateway
- Mobility Management Entity
- Home Subscriber Server

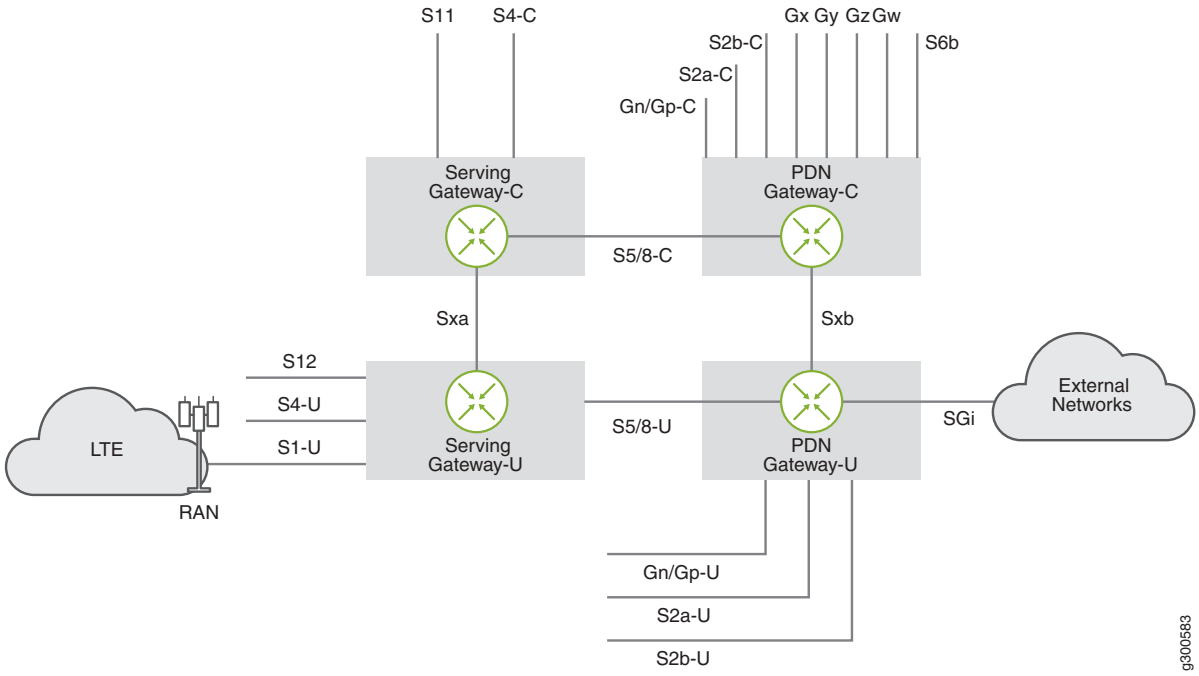
Figure 1: 3GPP Release 8 Evolved Packet Core Architecture



User Equipment (UE) has control and data path connectivity to the EPC network elements over eNodeB base stations. The EPC provides data connectivity to external networks such as the Internet.

3GPP Release 14 introduced CUPS. CUPS stands for Control and User Plane Separation, providing the architecture enhancements for the separation of functionality in the EPC's serving gateway (SGW) and PDN gateway (PGW). As Figure 2 on page 14 shows, both the serving gateway and the PDN gateway of the EPC can be separated into their control plane and user plane functions. CUPS introduces new interfaces, Sxa and Sxb, between the control plane and user plane functions of the SGW and PGW, respectively. CUPS enables control plane and user plane functions to be deployed, scaled and operated separately while integrated over a standard reference interface.

Figure 2: 3GPP Release 14 CUPS Architecture



The control plane provides the following functionality:

- Receives traffic rules and actions
- Triggers accounting
- Makes session level announcements
- Receives usage information
- Receives user plane status information
- Northbound integration with the signaling plane
- Configures and enables Lawful Intercept sessions

The user plane provides the following functionality:

- Subscriber tunnel encapsulations (GTP-U)
- Packet routing and forwarding
- QoS and buffering
- Policy enforcement
- Statistics gathering and reporting
- Enacts Lawful Intercept requests
- Optional advanced services

With this functional separation, the control plane and user plane have very distinct deployment requirements and can be in different physical locations. While the control plane function is very complex, the user plane function requires high packet processing capability and rich policy enforcement. The user plane can be more distributed than the control plane and located closer to end-user access points, such as a radio access network (RAN), enabling higher bandwidth per user while delivering lower latency. Control plane and user plane separation provides the following benefits:

- Independent scaling of the user and control planes.
- Network architecture flexibility including:
  - Ability to deploy from the edge to the core.
  - Ability to segregate different traffic types and services across different user planes while maintaining a common or single control plane.
- Operational flexibility
- Easier migration path from 4G to 5G services. CUPS is optional for 4G, but is an integral part of the 5G network architecture.

The Junos Multi-Access User Plane solution is to provide a combined SGW user plane (SGW-U) and PGW user plane (PGW-U) in a single MX series router (see Figure 3 on page 15). The combined SGW-U/PGW-U is referred to as a SAEGW-U (System Architecture Evolution Gateway-User Plane). Juniper's MX SAEGW-U can interoperate with a third-party combined SGW-C/PGW-C, hereafter referred to as SAEGW-C, through a combined Sxa/Sxb interface.

> **NOTE:** Juniper's MX SAEGW-U communicates with the third-party SAEGW-C over the Sxa/Sxb interface through Packet Forwarding Control Protocol (PFCP) as specified in 3GPP TS 29.244.

Figure 3: Junos Multi Access User Plane SAEGW-U

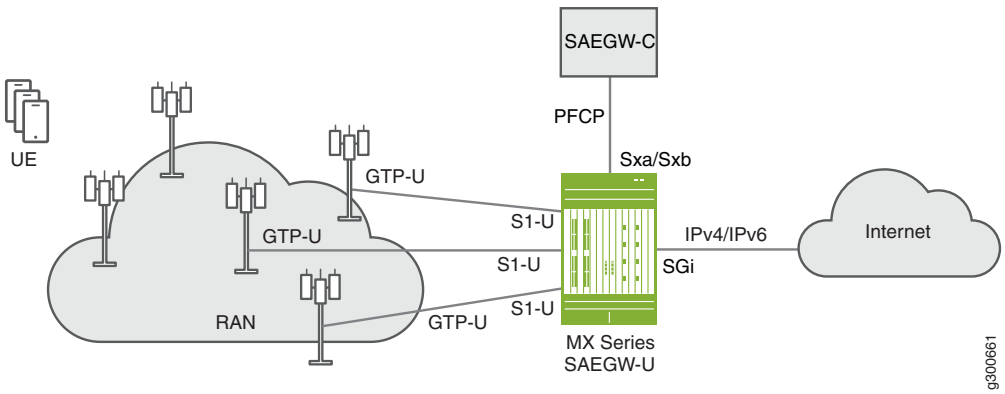


Table 3 on page 16 provides lists some useful terminology to help you understand the Junos Multi Access User Plane.

Table 3: Terminology for Junos Multi-Access User Plane

Term	Description
3GPP	The 3rd Generation Partnership Project is an international standards organization that develops specifications and protocols for wireless telephony.
APN	The access point name identifies the packet data network (PDN), such as the Internet, that the subscriber wants to access. When a subscriber requests access, the UE passes the requested APN to the eNodeB, which sends it to the MME for authorization. If the subscriber does not request an APN, the MME can authorize a default APN. Each PDN that the user subscribes to has an APN and an associated SAEGW-U that the UE uses to access the PDN. The combination of APN and SAEGW-U is called a PDN subscription context. One context is the default APN, which always connects to a PDN such as the Internet unless the user activates another APN. The HSS maintains subscriber profiles, The MME uses the profile from the HSS to validate whether the subscriber is actually subscribed to the requested APN. You can also think of the APN as the set of service-level and connection parameters—such as QoS parameters—that is authorized for the UE. A given UE can access many APNs. An APN has two parts: • Network Identifier—This defines the external PDN that the user connects to through a SAEGW-U. This part of the APN is mandatory. It can be as simple as internet or have a more complicated structure such as example.net. The network identifier can optionally specify a requested subscriber service. Operator Identifier—(Optional) This defines the provider whose PDN the user connects to through a SAEGW-U. This part of the APN is often omitted. If present, it consists of the provider's Mobile Network Code (MNC) and Mobile Country Code (MCC). An APN that includes both a Network Identifier and an Operator Identifier corresponds to a DNS name for the SAEGW-U. The APN has the following format: *network-id*.mnc*mnc-number*.mcc*mcc-number.gprs* An APN can be a simple string or more complex, as shown in these examples: • fixed-wireless • web.example.net • internet.mnc99.mcc999.gprs

Table 3: Terminology for Junos Multi-Access User Plane *(continued)*

Term	Description
Bearer	An end-to-end bearer is the tunnel that connects the UE to a PDN through the SAEGW-U. A *default bearer* is established to a default SAEGW-U whenever the UE is activated. Activation means here that the UE is on and has performed authentication. A UE device has a default bearer for each SAEGW-U to which it connects. For example, if user equipment connects to the Internet through one SAEGW-U and a corporate intranet through another SAEGW-U, two default bearers will be active. Default bearers are best-effort. The UE can establish *dedicated bearers* to the SAEGW-U that can have different QoS requirements, such as a guaranteed bit rate (GBR).
eNodeB	The hardware (typically in a radio tower) that connects directly to the UE over the air and to the wireless network core. Also called evolved Node B or E-UTRAN Node B. Some of the eNodeB functions include: • Terminates the radio connection from the UE. • Locates the MME that authenticates the UE (SIM card) with information from the subscriber profile maintained on the HSS. Maintains S1-MME control plane connectivity. • Maintains the S1-U data plane interface with the SAEGW-U. An S1-U interface can support multiple eNodeBs.
GTP	The GPRS tunneling protocol governs the creation and use of GTP tunnels that carry traffic between two GPRS support nodes (GSNs). Each GTP tunnel is identified by a TEID. The receiving end of a tunnel assigns locally the TEID that the transmitting side uses. The tunnel endpoints on the nodes exchange messages to communicate the TEID values to each other.
GTP-C	The GPRS tunneling protocol, control plane. GTP-C tunnels carry packet data units and signaling messages in the control plane from eNodeBs to MMEs to the SAEGW-C.
GTP-U	The GPRS tunneling protocol, user plane. GTP-U tunnels carry packet data units and signaling messages in the user (data) plane (S1-U interface) between tunnel endpoints on the eNodeB and the SAEGW-U.
S11	The GTPv2-based control plane interface that connects the MME and the SAEGW-C. GTP-C tunnels carry control messages. An S11 interface can support multiple MMEs.
S1-MME	The GTPv2-based control plane interface that connects eNodeB and the MME.

Table 3: Terminology for Junos Multi-Access User Plane *(continued)*

Term	Description
S1-U	The GTPv1-based user plane interface that connects eNodeB and the SAEGW-U. S1-U is also called the data plane interface. GTP-U tunnels on the interface carry user payloads. An S1-U interface can support multiple eNodeBs.
SAEGW	The System Architecture Evolution gateway that includes the functions of both the SGW and the PGW.
TEID	A tunnel endpoint identifier that uniquely identifies a GTP tunnel endpoint in the scope of a path. A fully qualified TEID consists of an IP address concatenated with a locally allocated identifier. Four TEIDs are defined, together they uniquely identify a default bearer session: • L-TEID-C consists of the IP address of the S11 interface on the SAEGW-C and the SAEGW-C's allocated identifier. • L-TEID-U consists of the IP address of the S1-U interface on the SAEGW-U and the SAEGW-U's allocated identifier • R-TEID-C consists of the IP address of the S11 interface on the MME and the MME's allocated identifier. • R-TEID-U consists of the IP address of the S1-U interface on the eNodeB and the eNodeB's allocated identifier
UE	The user equipment that connects to the wireless network's eNodeB and to the subscriber's network. UE corresponds to what is called CPE in other contexts. In some cases, the UE consists of a SIM card and a residential gateway router (RG) that can host the SIM. In other cases the SIM might be in a separate device that connects to the RG.

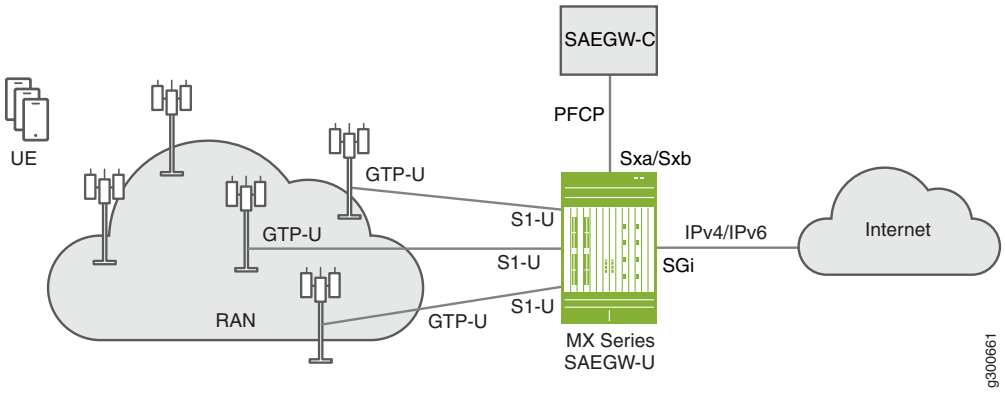
RELATED DOCUMENTATION

MX Series Router As SAEGW-U | **19**

MX Series Router As SAEGW-U

The Junos Multi-Access User Plane solution is to provide a combined SGW user plane (SGW-U) and PGW user plane (PGW-U) in a single MX series router. The combined SGW-U/PGW-U is referred to as a SAEGW-U (System Architecture Evolution Gateway-User Plane). As Figure 4 on page 19 shows, Juniper's MX SAEGW-U interoperates with a third-party SAEGW-C through a combined Sxa/Sxb interface.

Figure 4: MX Series SAEGW-U in the CUPS Wireless Network Architecture



The MX SAEGW-U supports the following CUPS interfaces:

- **Combined Sxa/Sxb**—A new protocol called Packet Forwarding Control Protocol (PFCP) enables communication on the Sxa/Sxb interface between the SAEGW-C and SAEGW-U. PFCP encodes TLV messages for transport over UDP/IP. The Sxa/Sxb interface can also transport user data packets (GTP-U based) between the user plane and control plane. SAEGW-U runs PFCP as the control protocol with the third-party SAEGW-C to set up data paths for wireless subscribers.
- **S1-U**—The S1-U interface is the data path between an eNodeB and the SAEGW-U. Application data packets from end-user equipment are encapsulated over GTP. For upstream packets, SAEGW-U is responsible for GTP tunnel termination and forwarding the user packets to the core. For downstream packets from core, SAEGW-U adds the GTP header and forwards to eNodeB(s). The data plane of SAEGW-U handles IP packets encapsulated in GTP-U from/ to eNodeBs that arrive for the mobile subscribers and performs routing to/from the external Internet.
- **SGi**—Interface to the core Internet, supporting both IPv4 and IPv6.

The MX SAEGW-U as the user plane provides the following functionality:

- Subscriber tunnel encapsulations (GTP-U)
- Packet routing and forwarding
- Bandwidth policing based on rules defined by the SAEGW-C

- Layer 3 policy enforcement based on policies defined by the SAEGW-C
- Statistics gathering and reporting for accounting and customer billing purposes
- Lawful intercept

The Junos Multi-Access User Plane solution is to provide purely the SAEGW-U in the form of an MX router that interacts with a third-party SAEGW-C. The MX router, functioning as an SAEGW-U, receives instructions from the SAEGW-C through the Sxa/Sxb interface using PFCP. Based on those instructions, the MX routing engine manages SAEGW-U sessions and programs data paths in the anchor PFEs. For the MX router to function as an SAEGW-U, it must contain the following minimum elements:

- **At least one anchor PFE interface**–An anchor PFE interface is a line card interface that has no physical interface connection, but rather provides the core processing of data traffic by doing the following:
  - Encoding/decoding of GTP-U packets. The anchor PFE interface decodes GTP-U packets from eNodeBs and forwards them to the core network and encodes IPv4/IPv6 packets from the core network and forwards them to eNodeBs.
  - Enforces class of service and firewall filter rules on subscriber sessions
  - Collects statistics on data usage for charging/accounting purpose
- **At least one signalling/control interface**-This is the Sxa/Sxb interface in the CUPS architecture. The signalling/control interface is a physical interface that does the following:
  - Sends/receives PFCP packets to/from the SAEGW-C
- **At least one ingress interface**-This is the S1-U interface in the CUPS architecture. The ingress interface is a physical interface that does the following:
  - Forwards GTP-U packets between eNodeBs and the anchor PFE
- **At least one egress interface**-This is the SGi interface in the CUPS architecture. The egress interface is a physical interface that does the following:
  - Forwards IPv4/IPv6 packets between the anchor PFE and the core network

> **NOTE:** You can configure all four interface types on the same line card, as long as that line card supports all of the interface types. See Table 4 on page 21.

Table 4 on page 21 describes the hardware and software requirements for the Junos Multi-Access User Plane solution.

Table 4: Junos Multi-Access User Plane Platform Support

Junos OS Release	Supported Platforms	Line Cards Supporting Anchor PFE Interfaces	Line Cards Supporting Signalling, Ingress, and Egress Interfaces	Supported Routing Engines
Starting in Junos OS Release 19.4R1	• MX240 • MX480 • MX960	• MPC7	• MPC2 • MPC3 • MPC4 • MPC5 • MPC7	• RE-S-1800X4-32G-S • RE-S-X6-64G-S • RE-S-X6-128G
Starting in Junos OS Release 20.2R1	• MX204 • MX10003	MX10003 MPC (Multi-Rate)	MX10003 MPC (Multi-Rate)	

NOTE: One MPC7 line card contains up to two anchor PFE interfaces.

NOTE: MX204 routers do not support GRES or APFE redundancy.

Table 5 on page 21 lists the maximum number of sessions and bearers each platform can support as an SAEGW-U.

Table 5: Scaling Support per Platform as SAEGW-U

Platform	Sessions	Bearers
MX204	100,000	200,000
MX240/MX480/MX960	1 Million	2 Million
MX10003	500,000	1 Million

Table 6 on page 21 lists the 3GPP technical specifications for Junos Multi-Access User Plane.

Table 6: 3GPP Technical Specifications for Junos Multi-Access User Plane

Specification Number	Specification Title
3GPP TS 23.007	Restoration procedures
3GPP TS 23.203	Policy and charging control architecture
3GPP TS 23.214	Architecture enhancements for control and user plane separation of EPC nodes

Table 6: 3GPP Technical Specifications for Junos Multi-Access User Plane *(continued)*

Specification Number	Specification Title
3GPP TS 23.401	General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
3GPP TS 29.244	Interface between the Control Plane and the User Plane nodes
3GPP TS 29.281	General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)
3GPP TS 33.107	Lawful interception architecture and functions **NOTE:** There is nothing to configure on the MX SAEGW-U to support Lawful Intercept except a loopback address. The SAEGW-U receives Lawful Intercept configuration information from the SAEGW-C through the Sxa/Sxb interface. When Lawful Interfcept is enabled, the SAEGW-U duplicates the client session bearer data traffic and forwards the intercepted packets to the SX3LIF through the X3u interface using GTP-U encapsulation.

RELATED DOCUMENTATION

Configuring an MX Router as an SAEGW-U | 39

CUPS Session Creation and Data Flow with Junos Multi-Access User Plane

IN THIS SECTION

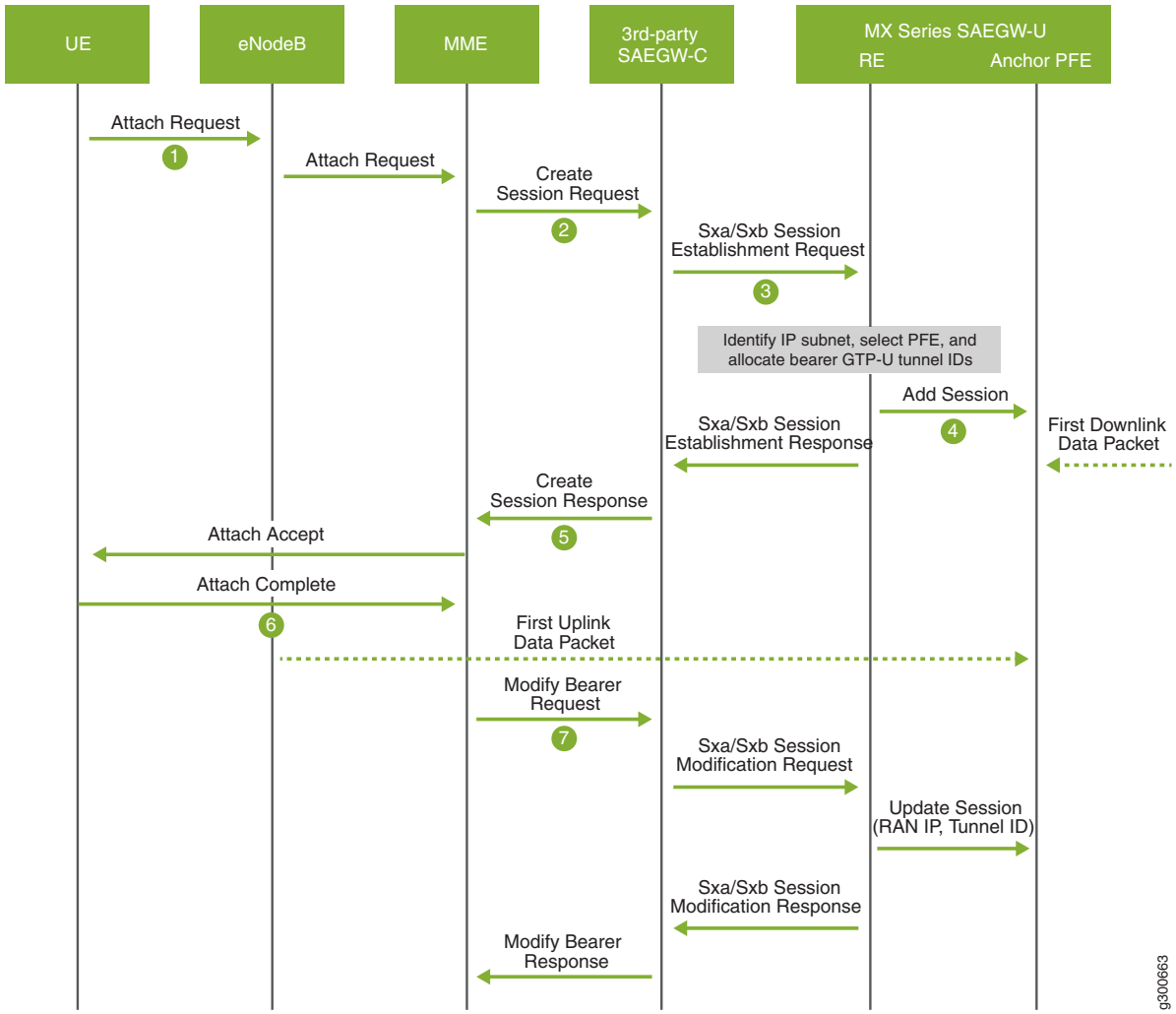
With the introduction of CUPS, it's useful to illustrate how an end-user session is created, how data flows during the session, and how the session is terminated with Junos Multi-Access User Plane.

CUPS Session Creation

> **NOTE:** Before a CUPS session can be created, the SAEGW-C must create and Sx association with the SAEGW-U. The SAEGW-C sends a Sx Association Setup Request message and the SAEGW-U responds with a Sx Association Setup Response message to create the association. Once this is done, the SAEGW-C can create Sx sessions on the SAEGW-U.

When an end user wants to access the network, a CUPS session must be created. Figure 5 on page 23 illustrates this process once an Sx association is established between the SAEGW-C and the SAEGW-U.

Figure 5: CUPS Session Creation



1. The user equipment (UE) sends an Attach Request to the eNodeB, which forwards the message to the mobility management entity (MME). The request includes the APN.

2. The MME sends a Create Session Request to the SAEGW-C.

3. The SAEGW-C performs the following actions:
   - Validates information elements received in the request.
   - Validates the APN requested by the subscriber.
   - Sends a Sxa/Sxb Session Establishment Request to the routing engine (RE) of the MX SAEGW-U.

   > **NOTE:** Sx session establishment is the SAEGW-C messaging the SAEGW-U control parameters on how to behave when the SAEGW-U encounters certain traffic. The minimum control parameters for Sx session establishment are one packet detection rule (PDR) and one forwarding action rule (FAR) The Sx session establishment effectively logs in the subscriber.

4. The RE of the SAEGW-U performs the following actions:
   - Identifies the IP address for the session.
   - Selects and anchor PFE to use for the session.
   - Allocates the bearer GTP-U tunnel IDs.
   - Adds the session to the anchor PFE.
   - Sends a Sxa/Sxb Session Establishment Response back to the SAEGW-C.
5. The SAEGW-C sends a Create Session Response back to the MME.

6. The MME sends an Attach Accept message to the UE, which responds with an Attach Complete message.

7. The MME sends a Modify Bearer request to the SAEGW-C, which sends an Sxa/Sxb Session Modification Request to the RE on the SAEGW-U. The RE updates the session IP address and tunnel ID of the eNodeB. Finally, a Modify Bearer Response is routed back to the MME.

NOTE: Sx Session Modification Request is the SAEGW-C messaging the SAEGW-U to modify any of the following four rules:

- Packet Detection Rule (PDR): contains information describing which packets should receive which treatment (for example, forwarding and other types of enforcement)
- Forwarding Action Rule (FAR): contains information on whether forwarding, dropping, or buffering is applied to a packet
- Usage Reporting Rule (URR): contains information that defines a certain measurement to make on user traffic and how that measurement shall be reported
- Quality Enforcement Rule (QER): contains information related to QoS enforcement of traffic

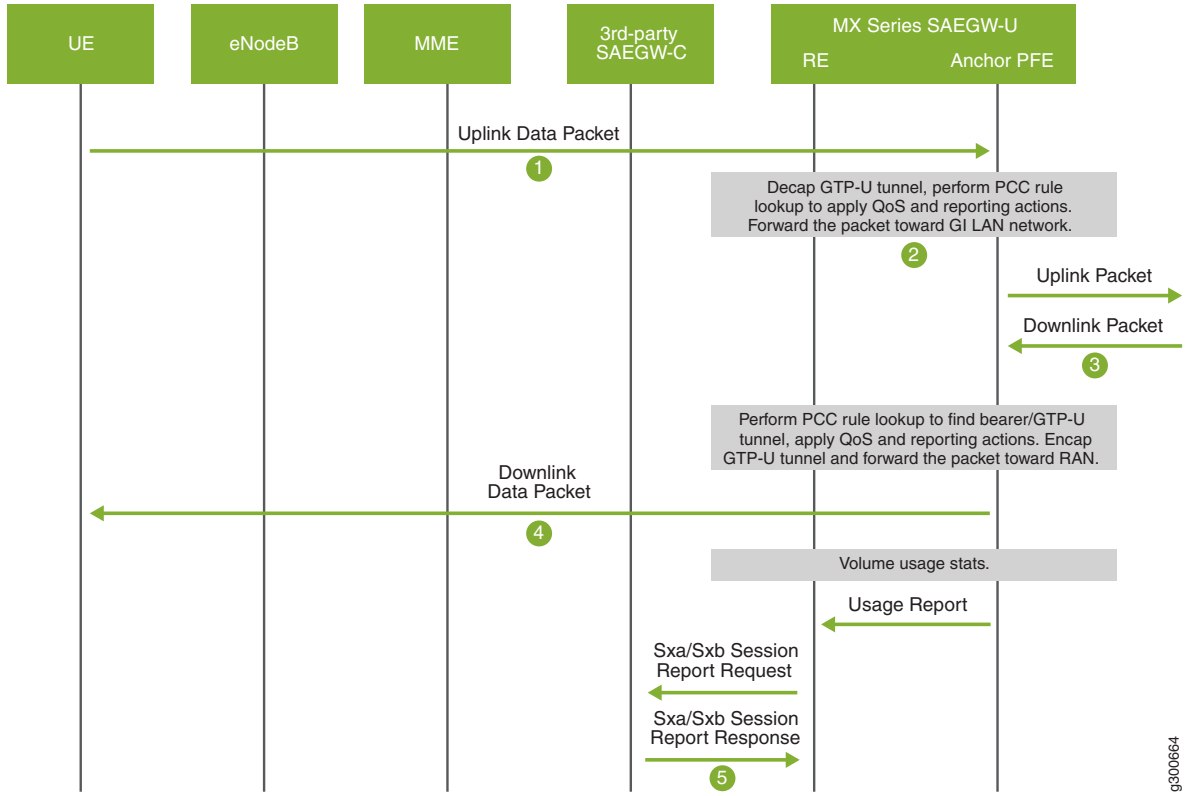
Junos Multi-Access User Plane does not support Buffering Action Rules (BARs).

8. The default bearer is now active and subscriber data traffic can pass back and forth between the UE through the eNodeB to the SAEGW-U and then the core network.

CUPS Session Data Flow

Once the session is established, the SAEGW-C is no longer directly involved for data flow. Data flows directly back and forth from the UE through the eNodeB to the SAEGW-U and then the core network. See Figure 6 on page 26.

Figure 6: CUPS Session Data Flow



1. The UE sends data to the eNodeB, which encodes the data as a GTP-U packet and forwards that packet to the anchor PFE on the SAEGW-U.

2. The anchor PFE of the SAEGW-U performs the following actions:
   - Decapsulates the GTP-U packet.
   - Performs PCC rule lookup to apply QoS and reporting actions.
   - Forwards the decapulated IPv4/IPv6 packet to the core network over the SGi interface.
3. The SAEGW-U receives a downlink IPv4/IPv6 packet from the core network.

4. The anchor PFE performs the following actions:

- Performs PCC rule lookup to determine the bearer GTP-U tunnel.
- Applies QoS and reporting actions.
- Encapsulates the IPv4/IPv6 packet in GTP-U.
- Forwards the GTP-U packet to the eNodeB, which decapsulates the packet and forwards the data to the UE.

5. The SAEGW-U also creates a usage report for the session and sends the report to the SAEGW-C over the Sxa/Sxb interface.

Charging and Usage Reports

Junos Multi Access User Plane supports charging and usage reports according to 3GPP TS 23.203, Policy and charging control architecture. Junos Multi Access User Plane supports the following usage reports:

- Volume threshold only
- Volume quota only
- Volume threshold and volume quota

Junos Multi Access User Plane uses the following process to generate usage reports:

1. The SAEGW-U creates a rating group for each bearer (default or dedicated). Routing groups can be created per session data flow (SDF) or for an entire bearer consisting of many SDFs.

2. The SAEGW-C sends a Usage Reporting Rule (URR) ID over the Sx interface.

3. The SAEGW-U associates the URR ID with a rating group.

4. The SAEGW-C also messages what type of report needs to be generated for the URR ID (volume threshold only, volume quota only, volume threshold and quota).

5. The default action when the volume quota is reached is to drop all traffic for the session data flow.

6. When the subscriber session ends, the SAEGW-U generates and sends a final usage report to the SAEGW-C.

RELATED DOCUMENTATION

GRES on Junos Multi-Access User Plane

Graceful Routing Engine switchover (GRES) in Junos OS enables a router with redundant Routing Engines to continue forwarding packets even if one Routing Engine fails. GRES preserves interface and kernel information. Traffic is not interrupted.

> **NOTE:** MX204 routers do not support GRES.

To preserve routing during a switchover, GRES must be combined with either:

- Graceful restart protocol extensions
- Nonstop active routing (NSR)

For Junos Multi-Access User Plane, GRES switchover protects the PFCP KeepAlive protocol. The new master Routing Engine starts answering peer keepalives.

Any updates to the master Routing Engine are replicated to the backup Routing Engine as soon as they occur.

Mastership switches to the backup Routing Engine if:

- The master Routing Engine kernel stops operating.
- The master Routing Engine experiences a hardware failure.
- The administrator initiates a manual switchover.

> **NOTE:** To quickly restore or to preserve routing protocol state information during a switchover, GRES must be combined with either graceful restart or nonstop active routing, respectively. For more information about graceful restart, see *Graceful Restart Concepts*. For more information about nonstop active routing, see *Nonstop Active Routing Concepts*.

If the backup Routing Engine does not receive a keepalive from the master Routing Engine after 2 seconds, it determines that the master Routing Engine has failed; and assumes mastership.

The Packet Forwarding Engine:

- Seamlessly disconnects from the old master Routing Engine
- Reconnects to the new master Routing Engine
- Does not reboot
- Does not interrupt traffic

The new master Routing Engine and the Packet Forwarding Engine then become synchronized. If the new master Routing Engine detects that the Packet Forwarding Engine state is not up to date, it resends state update messages.

NOTE: Successive Routing Engine switchover events must be a minimum of 240 seconds (4 minutes) apart after both Routing Engines have come up.

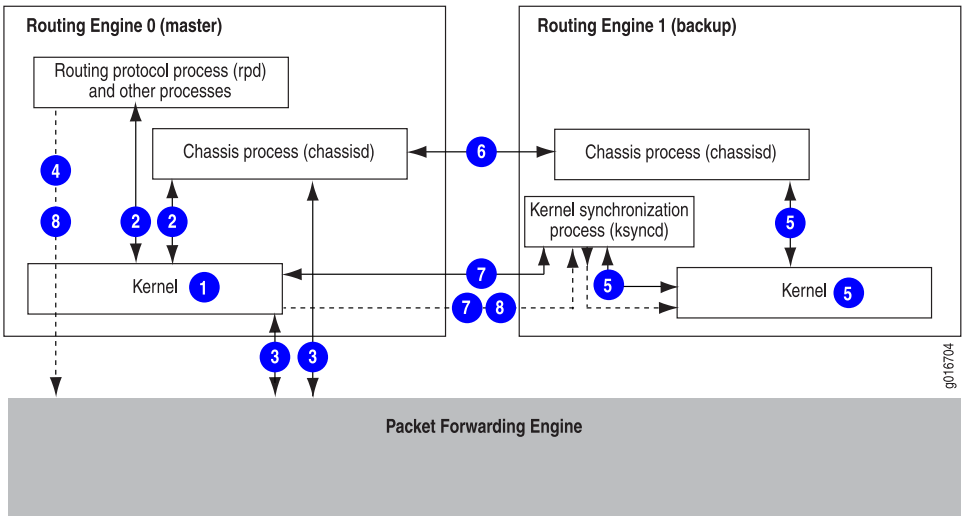
If the router or switch displays a warning message similar to **Standby Routing Engine is not ready for graceful switchover. Packet Forwarding Engines that are not ready for graceful switchover might be reset** , do not attempt switchover. If you choose to proceed with switchover, only the Packet Forwarding Engines that were not ready for graceful switchover are reset. None of the FPCs should spontaneously restart. We recommend that you wait until the warning no longer appears and then proceed with the switchover.

NOTE:

- We do *not* recommend performing a commit operation on the backup Routing Engine when GRES is enabled on the router or switch.
- We do *not* recommend enabling GRES on the backup Routing Engine in *any* scenario.

Figure 7 on page 29 shows the system architecture of graceful Routing Engine switchover and the process a routing platform follows to prepare for a switchover.

Figure 7: Preparing for a Graceful Routing Engine Switchover



NOTE: Check GRES readiness by executing both:

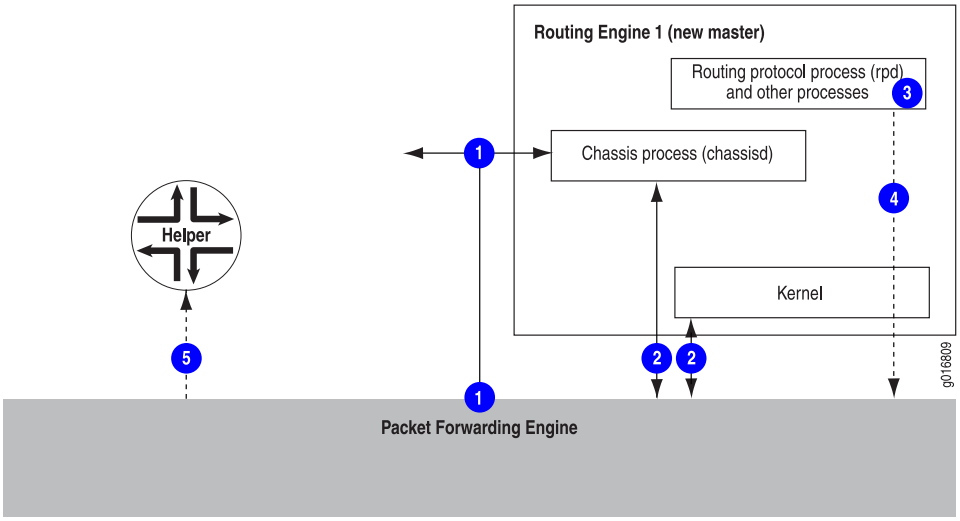
- The **request chassis routing-engine master switch check** command from the master Routing Engine
- The **show system switchover** command from the Backup Routing Engine

The switchover preparation process for GRES is as follows:

1. The master Routing Engine starts.
2. The routing platform processes (such as the chassis process [chassisd]) start.
3. The Packet Forwarding Engine starts and connects to the master Routing Engine.
4. All state information is updated in the system.
5. The backup Routing Engine starts.
6. The system determines whether GRES has been enabled.
7. The kernel synchronization process (ksyncd) synchronizes the backup Routing Engine with the master Routing Engine.
8. After ksyncd completes the synchronization, all state information and the forwarding table are updated.

Figure 8 on page 30 shows the effects of a switchover on the routing (or switching)platform.

Figure 8: Graceful Routing Engine Switchover Process



A switchover process consists of the following steps:

1. When keepalives from the master Routing Engine are lost, the system switches over gracefully to the backup Routing Engine.
2. The Packet Forwarding Engine connects to the backup Routing Engine, which becomes the new master.
3. Routing platform processes that are not part of GRES (such as the routing protocol process rpd) restart.
4. State information learned from the point of the switchover is updated in the system.
5. If configured, graceful restart protocol extensions collect and restore routing information from neighboring peer *helper* routers.

NOTE: For MX Series routers using enhanced subscriber management, the new backup Routing Engine (the former master Routing Engine) will reboot when a graceful Routing Engine switchover is performed. This cold restart resynchronizes the backup Routing Engine state with that of the new master Routing Engine, preventing discrepancies in state that might have occurred during the switchover.

NOTE: In Junos Multi-Access User Plane configuration, if the mobile-edge configuration is committed and then GRES needs to be enabled or disabled, a reboot of the entire chassis is required.

NOTE: In Junos Multi-Access User Plane, any subscriber session whose Session State is *not* **ESTABLISHED**, a graceful restart logs out that subscriber and cleans up any state. The SAEGW-C will need to reestablish this session

Table 7: Effects of a Routing Engine Switchover

Feature	Benefits	Considerations
Dual Routing Engines only (no features enabled)	• When the switchover to the new master Routing Engine is complete, routing convergence takes place and traffic is resumed.	• All physical interfaces are taken offline. • Packet Forwarding Engines restart. • The backup Routing Engine restarts the routing protocol process (rpd). • All hardware and interfaces are discovered by the new master Routing Engine. • The switchover takes several minutes. • All of the router's adjacencies are aware of the physical (interface alarms) and routing (topology) changes.
GRES enabled	• During the switchover, interface, mobile-edge subscriber information, and kernel information is preserved. • The switchover is faster because the Packet Forwarding Engines are not restarted.	• The new master Routing Engine restarts the routing protocol process (rpd). • All hardware and interfaces are acquired by a process that is similar to a warm restart. • All adjacencies are aware of the router's change in state. • Mobile-edge PFCP peer is not aware that GRES happened.
GRES *and* NSR enabled	• Traffic is not interrupted during the switchover. • Interface, mobile-edge subscriber information, and kernel information are preserved.	• Unsupported protocols must be refreshed using the normal recovery mechanisms inherent in each protocol. • Mobile-edge PFCP peer is not aware that GRES happened.

Table 7: Effects of a Routing Engine Switchover *(continued)*

Feature	Benefits	Considerations
GRES *and* graceful restart enabled	• Traffic is not interrupted during the switchover. • Interface, mobile-edge subscriber information, and kernel information are preserved. • Graceful restart protocol extensions quickly collect and restore routing information from the neighboring routers.	• Neighbors are required to support graceful restart, and a wait interval is required. • The routing protocol process (rpd) restarts. • For certain protocols, a significant change in the network can cause graceful restart to stop. • Starting with Junos OS Release 12.2, if adjacencies between the restarting router and the neighboring peer 'helper' routers time out, graceful restart can stop and cause interruptions in traffic. • Mobile-edge PFCP peer is not aware that GRES happened.

Release History Table

Release	Description
12.2	Starting with Junos OS Release 12.2, if adjacencies between the restarting router and the neighboring peer 'helper' routers time out, graceful restart can stop and cause interruptions in traffic.

RELATED DOCUMENTATION

Understanding Graceful Routing Engine Switchover

Configuring Graceful Routing Engine Switchover

Anchor PFEs and Redundancy in Junos Multi-Access User Plane

IN THIS SECTION

Understanding the Anchor PFE

An anchor PFE is the Packet Forwarding Engine (PFE) on a standard line card that has no direct interface connections, but rather provides the core processing of data traffic by doing the following:

- Encoding/decoding of GTP-U packets. The anchor PFE decodes GTP-U packets from eNodeBs and forwards them to the core network and encodes IPv4/IPv6 packets from the core network and forwards them to eNodeBs.
- Enforces class of service and firewall filter rules on subscriber sessions.
- Collects statistics on data usage for charging/accounting purpose.

Following are important points to consider when setting up anchor PFEs:

- You must configure at least one anchor PFE line card. We recommend at least two with 1:1 hot-standby redundancy.
- Each anchor PFE requires a defined **pfe-** interface of the form **pfe-x/y/z**.

Configuring No Redundancy for the Anchor PFEs

When no redundancy is required, all anchor PFE interfaces are equally available. The SAEGW-U uses all anchor PFE logical interfaces to anchor sessions/bearers. The routing engine (RE) of the SAEGW-U steers the GTP-U traffic for sessions and bearers to each of the anchor PFEs. The GTP processing for sessions and bearers and filter processing happens on the respective anchor PFE. The charging data is also maintained, collected and reported from the anchor for each session and its bearer.

When there is no redundancy configured, a failure of the anchor PFE line card is catastrophic for the SAEGW-U sessions/bearers in that control plane sessions corresponding to the failed anchor PFE and its data plane are lost. If supported by the SAEGW-C, the SAEGW-U can send an **Sx Session Set Deletion Request** for the lost sessions through the Sx interface, and the sessions are flushed in the SAEGW-C. All charging and other accounting data is lost for the sessions and bearers. New sessions can come up on the failed anchor PFE interface *only* when all sessions are flushed in the SAEGW-C for the failed anchor PFE, even if the anchor PFE comes up sooner. If other anchor PFE interfaces are available, new sessions can come up instantly on those anchor PFE interfaces.

Following is a typical configuration for two anchor PFEs with no redundancy.

1. Configure slot 1 & slot 2 for anchor processing.

```
[edit chassis]
user@host# set fpc 0 pfe 0 forwarding-packages mobility ggsn-pgw
user@host# set fpc 0 pfe 0 forwarding-packages mobility card-type-all
user@host# set fpc 1 pfe 0 forwarding-packages mobility ggsn-pgw
user@host# set fpc 1 pfe 0 forwarding-packages mobility card-type-all
```

2. Configure interfaces in slot 1 & slot 2 for PFCP processing.

```
[edit services mobile-edge gateways gateway-name system]
user@host# set anchor-pfes interface pfe-0/0/0
user@host# set anchor-pfes interface pfe-1/0/0
```

Configuring 1:1 Hot-standby Redundancy for the Anchor PFEs

To have 1:1 PFE redundancy, an aggregated anchor PFE group can be formed as below using exactly two PFE logical interfaces from different slots:

- Aggregated Anchor PFE group 1 – pfe-0/0/0 (primary), pfe-1/0/0 (secondary)
- Aggregated Anchor PFE group 2 – pfe-0/1/0 (primary), pfe-1/1/0 (secondary)

You cannot have primary and secondary anchor PFEs on the same line card. For example, the following combination is not supported:

- Aggregated anchor PFE group 1 – pfe-0/0/0 (primary), pfe-1/1/0 (secondary)
- Aggregated anchor PFE group 2 – pfe-1/0/0 (primary), pfe-0/1/0 (secondary)

We also do not recommended configuring anchor PFEs on two separate line cards with their secondary anchor PFEs on just one line card. For examle:

- Aggregated anchor PFE group 1 – pfe-0/0/0 (primary), pfe-2/0/0 (secondary)
- Aggregated anchor PFE group 2 – pfe-1/0/0 (primary), pfe-2/1/0 (secondary)

When aggregated anchor PFE configuration is used, both the primary anchor PFE and secondary anchor PFE have the session state. But the routing engine (RE) steers the GTP-U traffic for sessions and bearers only to the primary anchor PFE. The GTP processing for sessions and bearers and filter processing happens on the primary anchor PFE. The charging data is also maintained, collected and reported from the primary anchor PFE. The secondary is in hot-standby mode and is ready for takeover only in the event of primary anchor PFE failure.

Given the considerable load that a single anchor PFE linecard can need to handle, a single anchor PFE linecard is limited to a maximum of two redundancy groups. You can configure a single anchor PFE for one of the following roles:

- Dedicated primary for one redundancy group
- Dedicated secondary for one redundancy group
- Primary for two redundancy groups
- Secondary for two redundancy groups

When 1:1 redundancy is operational, the redundancy interface process monitors the health of the primary and secondary anchor PFEs.

A secondary anchor PFE failure results in zero data plane traffic loss on the primary anchor PFE. All active sessions remain unaffected. New sessions can come up without any latency. When the secondary anchor PFE is restored, there is a catchup phase to program the already active sessions and bearers in the secondary anchor PFE. After this is completed, new sessions are programmed in the secondary anchor PFE in parallel to the primary anchor PFE. From this point forward, the secondary anchor PFE can take over anytime.

If the primary anchor PFE fails, the secondary anchor PFE starts handling traffic. It might take a few seconds to detect the failure of the primary anchor PFE and for the RE to re-route the GTP-U traffic to the secondary PFE. This delay results in traffic loss during the anchor PFE switchover. Additionally, there is a loss of any charging data not reported by the primary anchor PFE before it failed. Anchor PFE switchover does not affect active sessions/bearers. In-flight changes to sessions and bearers as well as new sessions being created during anchor PFE switchover are rolled back. If supported by the SAEGW-C, the SAEGW-U can send an **Sx Session Set Deletion Request** for the lost sessions through the Sx interface, and the sessions are flushed in the SAEGW-C. After the anchor PFE switchover, the configured primary anchor PFE can be restored, starting as a secondary anchor PFE and going through catch-up similar to secondary APFE failure and restoration described above.

To configure redundancy for two anchor PFE line cards:

1. Configure PFE interfaces in each anchor PFE line card slot in aggregated anchor PFE configuration. For example:

```
[edit interfaces]
user@host# set apfe0 anchoring-options primary-list pfe-0/0/0
user@host# set apfe0 anchoring-options secondary pfe-1/0/0
user@host# set apfe1 anchoring-options primary-list pfe-0/1/0
user@host# set apfe1 anchoring-options secondary pfe-1/1/0
```

2. Reference the aggregated anchor PFE interfaces in the SAEGW-U configuration. For example:

```
[edit services mobile-edge gateways gateway-name system]
user@host# set anchor-pfes interface apfe0
user@host# set anchor-pfes interface apfe1
```

When the configured primary anchor PFE fails, the secondary anchor PFE takes over. When the failed primary anchor PFE recovers, it does not automatically resume primary status. It is now in secondary status until the configured secondary anchor PFE fails.

1. However, you can force the two anchor PFEs to revert to their configured state by setting a **revert-time**, in hours, under the **[edit interfaces aggregated-pfe-group anchoring-options]** hierarchy. For example:

```
[edit interfaces]
user@host# set apfe0 anchoring-options revert-time 2
user@host# set apfe1 anchoring-options revert-time 2
```

RELATED DOCUMENTATION

Configuring an MX Router as an SAEGW-U | 39

2

CHAPTER

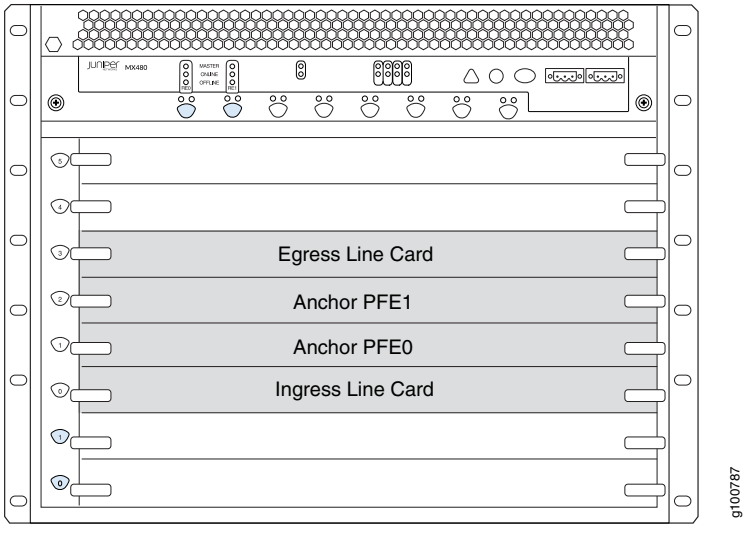
MX Series SAEGW-U Configuration

Configuring an MX Router as an SAEGW-U

IN THIS SECTION

As Figure 9 on page 39 shows, a standard setup of an MX Series router as an SAEGW-U includes an ingress line card, and egress line card, and a recommended two anchor PFE line cards operating redundantly.

Figure 9: Standard setup for MX Series router as SAEGW-U



- The ingress line card provides the S1-U interface, connecting to the radio access network (RAN), and the combined Sxa/Sxb interface, connecting to the SAEGW-C.
- The anchor PFE line cards provide the core processing of data traffic through internal **pfe-** interfaces. At least one anchor PFE card is required, but two are recommended to provide redundancy.

- The egress line card provides the SGi interface, connecting to the core Internet.
- You can configure all of this functionality on a single line card as long as that line card supports all of the SAEGW-U functionality. We show separate line cards here for simplicity and recommended setup.

To configure an MX router as an SAEGW-U, perform the following configuration procedures in the listed order:

GRES Configuration

The graceful Routing Engine switchover (GRES) feature in Junos OS enables a router with redundant Routing Engines to continue forwarding packets, even if one Routing Engine fails. GRES preserves interface and kernel information. Traffic is not interrupted.

1. Configure Graceful Restart (GRES).

```
[edit chassis]
user@host# set redundancy graceful-switchover
user@host# commit
```

SEE ALSO

GRES on Junos Multi-Access User Plane | 28

Chassis Configuration for the Anchor PFE Line Cards

Define each Packet Forwarding Engine (PFE) on each anchor PFE line card as an anchor interface.

1.

```
[edit chassis]
user@host# set fpc anchor-pfe0-slot pfe 0 forwarding-packages mobility ggsn-pgw
user@host# set fpc anchor-pfe0-slot pfe 0 forwarding-packages mobility card-type-all
user@host# set fpc anchor-pfe0-slot pfe 1 forwarding-packages mobility ggsn-pgw
user@host# set fpc anchor-pfe0-slot pfe 1 forwarding-packages mobility card-type-all
user@host# set fpc anchor-pfe1-slot pfe 0 forwarding-packages mobility ggsn-pgw
user@host# set fpc anchor-pfe1-slot pfe 0 forwarding-packages mobility card-type-all
user@host# set fpc anchor-pfe1-slot pfe 1 forwarding-packages mobility ggsn-pgw
user@host# set fpc anchor-pfe1-slot pfe 1 forwarding-packages mobility card-type-all
```

```
user@host# commit
```

Interface Configuration

Configure the interfaces needed for the SAEGW-U.

1. Define the SGi interface. This interface is on the egress line card.

   ```
   [edit interfaces]
   user@host# set SGi-interface-name unit 0 family inet address interface-address
   ```

2. Define the Sx interface, which connects to the SAEGW-C. This interface is on the ingress line card.

   ```
   [edit interfaces]
   user@host# set Sx-interface-name unit 0 family inet address interface-address
   ```

3. Define the S1-U interface, which connects to the access network. This interface is on the ingress line card and is set to admit only GTP packets.

   ```
   [edit interfaces]
   user@host# set S1-U-interface-name unit 0 family inet address interface-address
   user@host# set S1-U-interface-name unit 0 family inet filter input filter-name
   ```

4. Define the UPF local address and Mobile Edge interface.

   ```
   [edit interfaces]
   user@host# set lo0 unit 0 family inet address UPF-local-address
   user@host# set mif unit 0 family inet
   ```

   NOTE: If you are connecting to multiple SAEGW-Cs, define the local address under the **control-plane-peers** stanza for each SAEGW-C rather than define a single loopback address.

> **NOTE:** **mif.0** is used in the default **inet.0** routing instance. Junos OS creates a default APN with **inet.0** as the routing instance. If you want to configure other routing instances, you must create **mif** interfaces with unit numbers other than **0**.

5. Assuming two anchor PFE linecards, each with two PFEs, define the anchor PFE interfaces.

```
[edit interfaces]
user@host# set apfe0 anchoring-options primary-list pfe-pfe0-slot/0/0
user@host# set apfe0 anchoring-options secondary pfe-pfe1-slot/0/0
user@host# set apfe1 anchoring-options primary-list pfe-pfe0-slot/1/0
user@host# set apfe1 anchoring-options secondary pfe-pfe1-slot/1/0
user@host# commit
```

> **NOTE:** You cannot mix primary and secondary anchor PFEs on the same MPC. An MPC can have only either primary anchor PFEs or secondary anchor PFEs.

> **CAUTION:** Changing the anchor PFE redundancy configuration once sessions are active kills all active sessions.

Mobile Edge Configuration

Once you've configured all of the necessary interfaces, you can configure the MX router to be a SAEGW-U.

1. Configure the connection to the control plane, the SAEGW-C.

```
[edit services mobile-edge gateways saegw gateway-name control-plane-peers]
user@host# set local-address local-address
user@host# set apn-services apns apn-name mobile-interface mif.0
user@host# set peer-groups group-name path-management enable
user@host# set peer-groups group-name heartbeat-interval seconds
user@host# set peer-groups group-name n3-requests n3-requests
user@host# set peer-groups group-name t3-response seconds
user@host# set peer-groups group-name peer-address remote-peer-address
user@host# set peer-groups group-name peer-hostname remote-peer-hostname
```

> **NOTE:** If you are connecting to multiple SAEGW-Cs, define the local address under the **control-plane-peers** stanza for each SAEGW-C. The loopback address, however, is still required for Lawful Intercept to function.

2. Configure the connection to the access network through the S1-U interface.

```
[edit services mobile-edge gateways saegw gateway-name access-network-peers]
user@host# set local-address local-address
user@host# set peer-groups group-name peer-address remote-peer-address
user@host# set peer-groups group-name peer-hostname remote-peer-hostname
```

3. Define the interfaces that will provide the anchor PFE functionality.

```
[edit services mobile-edge gateways saegw gateway-name system]
user@host# set anchor-pfes interface apfe0
user@host# set anchor-pfes interface apfe1
user@host# commit
```

Firewall Configuration

Define a firewall filter that discards all packets except GTP packets at the S1-U interface.

1. GTP packets are UDP packets that have a destination port of 2152. GTP prime packets have a destination port of 3386. Accept and count these packets:

```
[edit firewall filter filter-name term 1]
user@host# set from protocol udp
user@host# set from destination-port 2152
user@host# set from destination-port 3386
user@host# set then count filter-name
user@host# set then next-hop-index 16777220
```

2. Discard all other packets:

```
[edit firewall filter filter-name term 2]
user@host# set then count default
```

```
user@host# set accept
user@host# commit
```

RELATED DOCUMENTATION

Anchor PFEs and Redundancy in Junos Multi-Access User Plane | 34

Example: Configuring an MX Router as an SAEGW-U | 44

Example: Configuring an MX Router as an SAEGW-U

IN THIS SECTION

This example shows how to configure an MX Series Router as an SAEGW-U for the Junos Multi-Access User Plane solution.

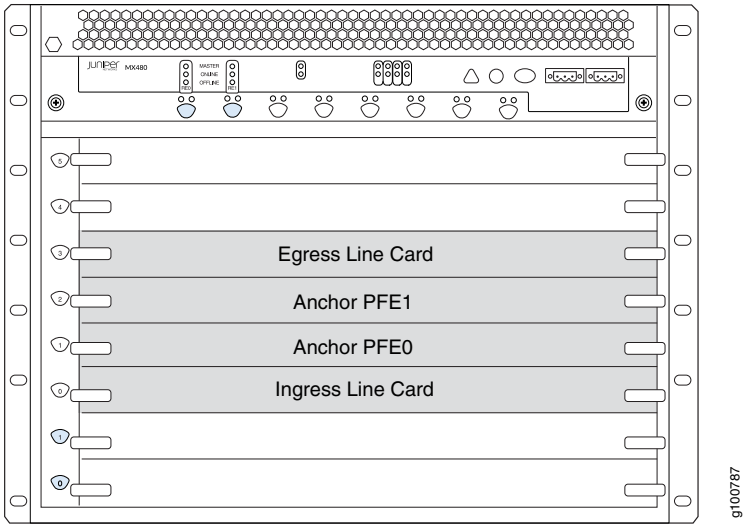
Requirements

This example uses the following hardware and software components:

- MX480 (can also be MX240, MX960) router with:
  - Two MPC7s to act as anchor packet forwarding engines (PFEs) to handle GTP-U processing
  - Two MPC2s (can also be MPC3, MPC5, MPC7, MPC10) to act as ingress and egress PFEs
- Junos OS Release 19.4R1 or later

Figure 10 on page 45 below shows the hardware for this example.

Figure 10: Standard setup for MX Series router as SAEGW-U



- The ingress line card (slot 0) provides the S1-U interface, connecting to the radio access network (RAN), and the combined Sxa/Sxb interface, connecting to the SAEGW-C.
- The anchor PFE line cards (slots 1 and 2) provide the core processing of data traffic through internal **pfe-** interfaces. At least one anchor PFE card is required, but two are recommended to provide redundancy.
- The egress line card (slot 3) provides the SGi interface, connecting to the core Internet.

Before you configure the MX Series Router as an SAEGW-U for the Junos Multi-Access User Plane solution, be sure you have:

- At least one configured SAEGW-C that you provide
- At lease one eNodeB
- Access to a packet data network (PDN)

Overview

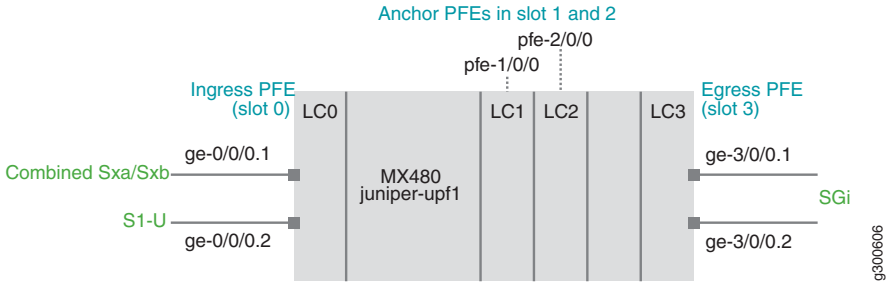
Topology

In this example (see Figure 11 on page 46):

- An MPC2 is in slot 0 with ge-0/0/0.1 providing the combined Sxa/Sxb interface and ge-0/0/0.2 providing the S1-U interface.

- MPC7s are in slots 1 and 2 to provide the anchor PFE interfaces.
- And MPC2 is in slot 3 with ge-3/0/0.1 and ge-3/0/0.2 providing SGi interfaces.

Figure 11: Configuring an MX Router as an SAEGW-U



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set chassis redundancy graceful-switchover
set chassis fpc 1 pfe 0 forwarding-packages mobility ggsn-pgw
set chassis fpc 1 pfe 0 forwarding-packages mobility card-type-all
set chassis fpc 2 pfe 1 forwarding-packages mobility ggsn-pgw
set chassis fpc 2 pfe 1 forwarding-packages mobility card-type-all
set interfaces ge-0/0/0 vlan-tagging
set interfaces ge-0/0/0 vlan-tagging unit 1 vlan-id 1
set interfaces ge-0/0/0 vlan-tagging unit 2 vlan-id 2
set interfaces ge-0/0/0 unit 1 family inet address 10.0.0.1/24
set interfaces ge-0/0/0 unit 2 family inet address 20.0.0.1/24
set interfaces ge-0/0/0 unit 2 family inet filter input gtpu-filter
set interfaces ge-3/0/0 vlan-tagging
set interfaces ge-3/0/0 vlan-tagging unit 1 vlan-id 1
set interfaces ge-3/0/0 vlan-tagging unit 2 vlan-id 2
set interfaces ge-3/0/0 unit 1 family inet address 30.0.0.1/24
set interfaces ge-3/0/0 unit 2 family inet address 30.0.0.1/24
set interfaces mif unit 0 family inet
set interfaces mif unit 1 family inet
set interfaces apfe0 anchoring-options primary-list pfe-1/0/0
```

```
set interfaces apfe0 anchoring-options secondary pfe-2/1/0
set services mobile-edge gateways saegw juniper-upf1 control-plane-peers local-address 10.0.0.1
set services mobile-edge gateways saegw juniper-upf1 control-plane-peers path-management enable
set services mobile-edge gateways saegw juniper-upf1 control-plane-peers heartbeat-interval 60
set services mobile-edge gateways saegw juniper-upf1 control-plane-peers apn-services apns apn-default
   mobile-interface mif.0
set services mobile-edge gateways saegw juniper-upf1 control-plane-peers apn-services apns apn-vrf1
   mobile-interface mif.1
set services mobile-edge gateways saegw juniper-upf1 access-network-peers local-address 20.0.0.1
set services mobile-edge gateways saegw juniper-upf1 system anchor-pfes interface apfe0
set routing-instances vrf1 instance-type virtual-router
set routing-instances vrf1 interface mif.1
set routing-instances vrf1 interface ge-3/0/0.2
set routing-instances vrf1 routing-options static route 0.0.0.0/0 next-table inet.0
set firewall filter gtpu-filter term 1 from protocol udp
set firewall filter gtpu-filter term 1 from destination-port 2152
set firewall filter gtpu-filter term 1 from destination-port 3386
set firewall filter gtpu-filter term 1 from destination-address 20.0.0.1
set firewall filter gtpu-filter term 1 then count gtpu
set firewall filter gtpu-filter term 1 then next-hop-index 16777220
set firewall filter gtpu-filter term 2 then count default
set firewall filter gtpu-filter term 2 then accept
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode*.

To configure the MX Router as an SAEGW-U:

1. Configure Graceful Restart (GRES).

```
[edit chassis]
user@host# set redundancy graceful-switchover
```

2. Configure slot 1 & slot 2 for anchor PFE processing.

```
[edit chassis]
user@host# set fpc 1 pfe 0 forwarding-packages mobility ggsn-pgw
user@host# set fpc 1 pfe 0 forwarding-packages mobility card-type-all
user@host# set fpc 2 pfe 1 forwarding-packages mobility ggsn-pgw
user@host# set fpc 2 pfe 1 forwarding-packages mobility card-type-all
```

3. Configure the ingress logical interfaces using vlans.

```
[edit interfaces ge-0/0/0]
user@host# set vlan-tagging
user@host# set vlan-tagging unit 1 vlan-id 1
user@host# set vlan-tagging unit 2 vlan-id 2
user@host# set vlan-tagging
user@host# set unit 1 family inet address 10.0.0.1/24
user@host# set unit 2 family inet address 20.0.0.1/24
user@host# set unit 2 family inet filter input gtpu-filter
```

4. Configure the egress PFE for routing to core/ Internet for subscriber in VRF default (apn1).

```
[edit interfaces ge-3/0/0]
user@host# set vlan-tagging unit 1 vlan-id 1
user@host# set vlan-tagging unit 2 vlan-id 2
user@host# set unit 1 family inet address 30.0.0.1/24
user@host# set unit 2 family inet address 30.0.0.1/24
```

5. Configure mobile interface for subscriber VRFs.

```
[edit interfaces mif]
user@host# set unit 0 family inet
user@host# set unit 1 family inet
```

6. Define the redundancy anchor PFE interfaces.

```
[edit interfaces]
user@host# set apfe0 anchoring-options primary-list pfe-1/0/0
user@host# set apfe0 anchoring-options secondary pfe-2/1/0
```

7. Define a name for the SAEGW-U gateway named **juniper-upf1**.

```
[edit services mobile-edge gateways]
user@host# set saegw juniper-upf1
```

8. Configure the address where PFCP peers will connect to the SAEGW-U. Also, configure two APNs for SAEGW-U (**apn-default** to place sessions in the default routing instance and **apn-vrf1** for sessions into **VRF1**).

```
[edit services mobile-edge gateways saegw juniper-upf1 control-plane-peers]
```

```
user@host# set local-address 10.0.0.1
user@host# set path-management enable
user@host# set heartbeat-interval 60
user@host# set apn-services apns apn-default mobile-interface mif.0
user@host# set apn-services apns apn-vrf1 mobile-interface mif.1
```

9. Configure the address where GTP-U peers will connect to the SAEGW-U.

```
[edit services mobile-edge gateways saegw juniper-upf1 access-network-peers]
user@host# set local-address 20.0.0.1
```

10. Configure aggregate interface **apfe0** for PFCP processing.

```
[edit services mobile-edge gateways saegw juniper-upf1 system]
user@host# set anchor-pfes interface apfe0
```

11. Configure the egress PFE for routing to core/ Internet for subscriber in VRF vrf1 (apn2).

```
[edit routing-instances vrf1]
user@host# set instance-type virtual-router
user@host# set interface mif.1
user@host# set interface ge-3/0/0.2
user@host# set routing-options static route 0.0.0.0/0 next-table inet.0
```

12. Define a firewall filter to direct GTP-u packets.

```
[edit firewall filter gtpu-filter]
user@host# set term 1 from protocol udp
user@host# set term 1 from destination-port 2152
user@host# set term 1 from destination-port 3386
user@host# set term 1 from destination-address 20.0.0.1
user@host# set term 1 then count gtpu
user@host# set term 1 then next-hop-index 16777220
user@host# set term 2 then count default
user@host# set term 2 then accept
```

Results

From configuration mode, confirm your configuration by entering the **show chassis**, **show interfaces**, **show services**, **show routing-instances**, **show unified-edge**, and **show firewall** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show chassis
redundancy {
    graceful-switchover;
}
fpc 1 {
    pfe 0 {
        forwarding-packages {
            mobility {
                ggsn-pgw;
                card-type-all;
            }
        }
    }
}
fpc 2 {
    pfe 1 {
        forwarding-packages {
            mobility {
                ggsn-pgw;
                card-type-all;
            }
        }
    }
}
```

```
user@host# show interfaces
ge-0/0/0 {
    vlan-tagging {
        unit-1 {
            vlan-id 1;
        }
        unit-2 {
            vlan-id 2;
        }
    }
    unit 1 {
        family inet {
```

```
            address 10.0.0.1/24;
        }
    }
    unit 2 {
        family inet {
            filter {
                input gtpu-filter;
            }
            address 20.0.0.1/24;
        }
    }
}
ge-3/0/0 {
    vlan-tagging {
        unit-1 {
            vlan-id 1;
        }
        unit-2 {
            vlan-id 2;
        }
    }
    unit 1 {
        family inet {
            address 30.0.0.1/24;
        }
    }
    unit 2 {
        family inet {
            address 30.0.0.1/24;
        }
    }
}
apfe0 {
    anchoring-options {
        primary-list {
            pfe-1/0/0;
        }
        secondary pfe-2/1/0;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 100.0.0.1/32;
```

```
        }
    }
}
mif {
    unit 0 {
        family inet;
    }
    unit 1 {
        family inet;
    }
}
```

```
user@host# show services
mobile-edge {
    gateways {
        saegw juniper-upf1 {
            system {
                anchor-pfes {
                    interface apfe0;
                }
            }
            control-plane-peers {
                local-address 10.0.0.1;
                path-management enable;
                heartbeat-interval 60;
                apn-services {
                    apns apn-default {
                        mobile-interface mif.0;
                    }
                    apns apn-vrf1 {
                        mobile-interface mif.1;
                    }
                }
            }
            access-network-peers {
                local-address 20.0.0.1;
            }
        }
```

```
    }
}
```

```
user@host# show firewall
filter gtpu {
    term 1 {
        from {
            protocol udp;
            destination-port [ 3386 2152 ];
        }
        then {
            count gtpu;
            next-hop-index 16777220;
        }
    }
    term 2 {
        then {
            count default;
            accept;
        }
    }
}
```

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

Verification

IN THIS SECTION

Use various **show** commands to verify the SAEGW-U is functioning properly.

Verify SAEGW-U State

Purpose

Verify the SAEGW-U is running and that GRES is enabled.

Action

```
user@host> show services mobile-edge summary
```

```
Graceful-Restart        Enabled
Mastership              Master
State                   Running
Bulk Sync               Synchronized
```

Verify SAEGW-U Peers

Purpose

Verify the SAEGW-U has connected and is communicating with the SAEGW-Cs (control peers) and eNodeBs (access peers).

Action

```
user@host> show services mobile-edge peers statistics
```

```
Peers Summary:
    Total control peers: 1
    Total access peers:  1
    Total association setup request rejects:  0

Control Peer Statistics:
    IP address:         13.1.0.4
    Hostname:           saegw-c1
    Routing-Instance:   default

    Heartbeat Requests Received:            11
    Heartbeat Responses Sent:               11

    Heartbeat Requests Sent:                2
    Heartbeat Responses Received:           2

    Association Setup Requests Received:    1
    Association Setup Responses Sent:       1
```

```
    Association Release Requests Received:   0
    Association Release Responses Sent:      0

    Session Establishment Requests Received: 30000
    Session Establishment Responses Sent (Accepted):    30000
    Session Establishment Responses Sent (Rejected):    0

    Session Modification Requests Received:             30000
    Session Modification Responses Sent (Accepted):     30000
    Session Modification Responses Sent (Rejected):     0

    Session Deletion Requests Received:                 23169
    Session Deletion Responses Sent (Accepted):         22968
    Session Deletion Responses Sent (Rejected):         0

Access Peer Statistics:
    IP address:         12.1.0.4
    Routing-Instance:   default

    Echo Requests Received:                 0
    Echo Responses Sent:                    0
    Echo Requests Sent:                     0
    Echo Responses Received:                0
```

Verify SAEGW-U Sessions

Purpose

Verify the SAEGW-U has active data sessions.

Action

`user@host>` **show services mobile-edge sessions summary**

```
Sessions by State:
    SESSION_WAIT: 35
    ESTABLISHED: 18561
    Total: 18596

Bearers by State:
    BEARER_WAIT: 30
```

```
    ESTABLISHED: 18561
    Total: 18591
```

user@host> **show services mobile-edge sessions**

```
    Session-address: 23.0.21.163 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-1/0/0 Secondary-anchor-PFE: apfe0:pfe-2/1/0
        Local-SEID: 0x20015a2 Remote-SEID: 0x3cb2

    Session-address: 23.0.47.237 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-1/0/0 Secondary-anchor-PFE: apfe0:pfe-2/1/0
        Local-SEID: 0x2fec Remote-SEID: 0x56fc

    Session-address: 23.0.21.49 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-1/0/0 Secondary-anchor-PFE: apfe0:pfe-2/1/0
        Local-SEID: 0x1531 Remote-SEID: 0x3c40

    Session-address: 23.0.29.83 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-1/0/0 Secondary-anchor-PFE: apfe0:pfe-2/1/0
        Local-SEID: 0x2001d53 Remote-SEID: 0x4462

....
```

RELATED DOCUMENTATION

- Anchor PFEs and Redundancy in Junos Multi-Access User Plane | 34
- Configuring an MX Router as an SAEGW-U | 39

3
CHAPTER

Configuration Statements

apn-services (SAEGW control plane services)

Syntax

```
apn-services {
    apns name {
        mobile-interface mobile-interface;
    }
}
```

Hierarchy Level

```
[edit services mobile-edge gateways saegw name control-plane-peers]
```

Release Information
Statement introduced in Junos OS Release 19.4R1.

Description
The access point name (APN) is sent by the SAEGW-C over PFCP to place a subscriber in a specific network instance.

Options
apn name—At least one access point name.

Required Privilege Level
system

forwarding-packages

Syntax

```
forwarding-packages {
    mobility {
        ggsn-pgw;
        sgw;
        card-type-all;
    }
}
```

Hierarchy Level

[edit chassis fpc *fpc-slot* pfe *pfe-id*]

Release Information
Statement introduced for Junos Multi-Acess User Plane in Junos OS Release 19.4R1.

Description

Configure the Packet Forwarding Engine so that it can be used to anchor mobile sessions. If this configuration is changed, then the FPC reboots.

The **forwarding-packages** statement can be configured at the Packet Forwarding Engine level. Therefore, you can configure a subset of Packet Forwarding Engines in an FPC to be mobile anchors.

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.

mobility

Syntax

```
mobility {
    ggsn-pgw;
    sgw;
    card-type-all;
}
```

Hierarchy Level

[edit chassis fpc *fpc-slot* pfe *pfe-id* forwarding-packages]

Release Information

Statement introduced for Junos Multi-Acess User Plane in Junos OS Release 19.4R1.

Description

Specify the forwarding package that the Packet Forwarding Engines associated with mobility must use.

NOTE:

- You must include every Packet Forwarding Engine configured with the **ggsn-pgw** forwarding package at the **[edit unified-edge gateways ggsn-pgw *gateway-name* system anchor-pfes]** hierarchy level on the broadband gateway. If you do not specify the Packet Forwarding Engine as an anchor interface, then the Packet Forwarding Engine will not be used by the broadband gateway.
- You must include every Packet Forwarding Engine configured with the **sgw** forwarding package at the **[edit unified-edge gateways sgw *gateway-name* system anchor-pfes]** hierarchy level on the broadband gateway. If you do not specify the Packet Forwarding Engine as an anchor interface, then the Packet Forwarding Engine will not be used by the broadband gateway.

Options

ggsn-pgw—Configure the router as a gateway GPRS support node (GGSN) or as a Packet Data Network Gateway (P-GW) or as an SAEGW-U.

sgw—Configure the router as a Serving Gateway (S-GW).

card-type-all—Required to configure the router as an SAEGW-U.

Required Privilege Level

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

RELATED DOCUMENTATION

forwarding-packages | 59

peer-groups (SAEGW access network peers)

Syntax

```
peer-groups name {
    peer {
        address [ address ... ];
        hostname hostname;
    }
    routing-instance routing-instance;
}
```

Hierarchy Level

[edit services mobile-edge gateways saegw *name* access-network-peers]

Release Information

Statement introduced in Junos OS Release 19.4R1.

Description

Peer-group name

Options

name—Peer group name.

peer—IPv4 address or prefix value (required) of the GTP-U peer and hostname (optional) of the GTP-U peer.

NOTE: The maximum number of peers that can appear in a peer group is 4000.

routing-instance—Routing-instance of a GPT-U peer.

NOTE: If at least one peer group is used, eNodeBs matching only this address/prefix are accepted by the SAEGW-U during session establishment. The eNodeB is bound to the routing instance within the **peer-groups** stanza, if available. Otherwise, the SAEGW-U uses the routing instance under **access-network-peers**.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system

peer-groups (SAEGW control plane peers)

Syntax

```
peer-groups name {
    heartbeat-interval seconds;
    n3-requests n3-requests;
    path-management (disable | enable);
    peer {
        address [ address ... ];
        hostname hostname;
    }
    routing-instance routing-instance;
    t3-response seconds;
}
```

Hierarchy Level

[edit services mobile-edge gateways saegw *name* control-plane-peers]

Release Information

Statement introduced in Junos OS Release 19.4R1.

Description

If at least one peer group is configured, PFCP packets from control plane peers matching this address/prefix alone are accepted. The control plane peers are bound to the routing instance defined within this peer group, if configured. Otherwise the control plane function is bound to the routing instance listed under control-plane-peers.

Options

name—Peer group name

heartbeat-interval—Time between origination of two successive heartbeat requests (seconds).

Range: 60 through 255

Default: 60

n3-requests—Maximim number of retries of PFCP request messages upon t3-response timeout.

Range: 1 through 5

Default: 3

path-management—Enable/disable origination of heartbeat message requests to control peers.

Default: Disabled

peer—IPv4 or IPv6 address or prefix value (required) of the PFCP peer and hostname (optional) of the PFCP peer.

routing-instance—Local routing instance of the PFCP peer.

t3-response—Waiting time of gateway before retrying a PFCP signaling-request upon response timeout (seconds).

Range: 1 through 5

Default: 5

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system

saegw

Syntax

```
saegw name {
    access-network-peers {
    ...}
    control-plane-peers {
    ...}
    system {
    ...}
}
```

Hierarchy Level

[edit services mobile-edge gateways]

Release Information

Statement introduced in Junos OS Release 19.4R1.

Description

Define the SAE gateway name.

> **NOTE:** Only a single instance of the SAE gateway can be defined on the MX Series router.

Options

name—SAE gateway name

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system

saegw access-network-peers

Syntax

```
access-network-peers {
    local-address [ local-address ... ];
    n3-requests n3-requests;
    peer-groups name {
        peer {
            address [ address ... ];
            hostname hostname;
        }
        routing-instance routing-instance;
    }
    routing-instance routing-instance;
    t3-response seconds;
}
```

Hierarchy Level

```
[edit services mobile-edge gateways saegw]
```

Release Information

Statement introduced in Junos OS Release 19.4R1.

Description

Use this section to define the connection to and characteristics of data plane peers.

Options

local-address—Required. IPv4 address(es) of the local end of the GTP-U connection.

NOTE: There is no limit to the number of data plane peers that can connect to the SAEGW-U.

n3-requests—Number of retries of peer management request messages upon **t3-response** timeout.

Range: 1 through 5

Default: 3

routing-instance—Local routing instance of the GTP-U connection.

NOTE: If at least one peer group is used, eNodeBs matching only the peer group address/prefix are accepted by the SAEGW-U during session establishment. The eNodeB is bound to the routing instance within the **peer-groups** stanza, if available. Otherwise, the SAEGW-U uses the routing instance provided here.

t3-response—Waiting time of SAEGW-U before retrying peer management request upon response timeout (seconds).

Range: 1 through 5

Default: 5

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system

saegw control-plane-peers

Syntax

```
control-plane-peers {
    apn-services {
        apns name {
            mobile-interface mobile-interface;
        }
    }
    heartbeat-interval seconds;
    local-address [ local-address ... ];
    n3-requests n3-requests;
    path-management (disable | enable);
    peer-groups name {
        heartbeat-interval seconds;
        initiate-association;
        n3-requests n3-requests;
        path-management (disable | enable);
        peer {
            address [ address ... ];
            hostname hostname;
        }
        routing-instance routing-instance;
        t3-response seconds;
    }
    response-cache-timeout seconds;
    routing-instance routing-instance;
    t3-response seconds;
}
```

Hierarchy Level

```
[edit services mobile-edge gateways saegw]
```

Release Information

Statement introduced in Junos OS Release 19.4R1.

Description

Use this section to define the connection to and characteristics of control plane peers (SAEGW-Cs).

Options

heartbeat-interval—Time between two successive heartbeat requests (seconds).

Range: 60 through 255

Default: 60

local-address—Required. IPv6 or IPv4 or both addresses of the local end of the PFCP connection.

> **NOTE:** If you are connecting to multiple SAEGW-Cs, define the local address under the **control-plane-peers** stanza for each SAEGW-C rather than define a single loopback address.

n3-requests—Maximim number of retries of PFCP request messages upon t3-response timeout.

Range: 1 through 5

Default: 3

path-management—Enable/disable origination of heartbeat message requests to control peers.

Default: Disabled

response-cache-timeout—Configure the timeout for the PFCP response cache (seconds).

Range: 0 through 255

Default: 0

routing-instance—Local routing instance of the PFCP. This is used to determine in which routing instance the responses are to be sent for incoming PFCP messages. If a routing instance is not configured:

- Only PFCP messages coming from control plane peers over the default routing instance are handled.
- PFCP responses are only sent in the default routing instance.
- PFCP messages coming over any other routing instance are dropped even if the destination address matches the defined **local-address**.

If a single routing instance is configured:

- Only PFCP messages coming from control plane peers over the configured routing instance are handled.
- PFCP responses are only sent through this routing instance.
- PFCP messages coming over any other routing instance are dropped.

t3-response—Waiting time of gateway before retrying a PFCP signaling-request upon response timeout (seconds).

Range: 1 through 5

Default: 5

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
system

saegw system

Syntax

```
system {
    anchor-pfes {
        interface interface-name;
    }
}
```

Hierarchy Level

```
[edit services mobile-edge gateways saegw]
```

Release Information

Description
Define the anchor PFEs for the SAEGW-U. The anchor PFEs are the line cards where the GTP-U data packets from **access-network-peers** are decapsulated and sent towards the SGi interface to the core network. Similarly, packets from the SGi interface are encapsulated in GTP-U by the anchor PFEs and sent towards the RAN.

Options
anchor-pfes —Define the anchor PFEs by providing their interface names.

Syntax: interface *interface-name*

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
system

CHAPTER 4

Operational Commands

show services mobile-edge peers

Syntax

```
show services mobile-edge peers
<statistics>
```

Release Information

Command introduced in Junos OS 19.4R1.

Description

This command gives information on SAEGW-C and access network peers known to the SAEGW-U.

Options

none—This command gives information on SAEGW-C and access network peers known to the SAEGW-U.

statistics—This command gives protocol statistics on SAEGW-C and access network peers known to the SAEGW-U.

Required Privilege Level

view

RELATED DOCUMENTATION

Example: Configuring an MX Router as an SAEGW-U | 44

List of Sample Output

show services mobile-edge peers on page 74
show services mobile-edge peers statistics on page 75

Output Fields

Table 8 on page 73 describes the output fields for the **show services mobile-edge peers** command. Output fields are listed in the approximate order in which they appear.

Table 8: show services mobile-edge peers Output Fields

Field Name	Field Description
Peers Summary	The **Peers Summary** field provides the following information: • Total number of control (SAEGW-C) peers. • Total number of access network peers. • Total rejected association setup requests.

Table 8: show services mobile-edge peers Output Fields *(continued)*

Field Name	Field Description
Control Peer Information	The **Control Peer Information** field provides the following information about each SAEGW-C: • IP address • Hostname • Routing-Instance • Peer Group name
Access Peer Information	The **Access Peer Information** field provides the following information about each access network peer: • IP address • Hostname • Routing-Instance • Peer Group name
Control Peer Statistics	The **Control Peer Statistics** field provides the following statistics about each SAEGW-C: • Heartbeat requests received and sent • Association setup requests received and sent • Association release requests received and sent • Session establishment requests received and sent (accepted and rejected) • Session modification requests received and sent (accepted and rejected) • Session deletion requests received and sent (accepted and rejected)
Access Peer Statistics	The **Access Peer Statistics** field provides the following statistics about each access network peer: • Echo requests received and sent

Sample Output

show services mobile-edge peers

`user@host>` **show services mobile-edge peers**

```
Peers Summary:
    Total control peers: 1
    Total access peers:  1
    Total association setup request rejects:  0
```

```
Control Peer information:
    IP address:          30.71.1.3
    Routing-Instance:    default

Access Peer information:
    IP address:          40.71.1.2
    Routing-Instance:    default
```

show services mobile-edge peers statistics

`user@host>` **show services mobile-edge peers statistics**

```
Peers Summary:
    Total control peers: 1
    Total access peers:  1
    Total association setup request rejects:  0

Control Peer Statistics:
    IP address:         13.1.0.4
    Hostname:           saegw-c1
    Routing-Instance:   default

    Heartbeat Requests Received:             11
    Heartbeat Responses Sent:                11

    Heartbeat Requests Sent:                 2
    Heartbeat Responses Received:            2

    Association Setup Requests Received:     1
    Association Setup Responses Sent:        1

    Association Release Requests Received:   0
    Association Release Responses Sent:      0

    Session Establishment Requests Received: 30000
    Session Establishment Responses Sent (Accepted):    30000
    Session Establishment Responses Sent (Rejected):    0

    Session Modification Requests Received:             30000
    Session Modification Responses Sent (Accepted):     30000
    Session Modification Responses Sent (Rejected):     0

    Session Deletion Requests Received:                 23169
```

```
    Session Deletion Responses Sent (Accepted):         22968
    Session Deletion Responses Sent (Rejected):         0

Access Peer Statistics:
    IP address:         12.1.0.4
    Routing-Instance:   default

    Echo Requests Received:                 0
    Echo Responses Sent:                    0
    Echo Requests Sent:                     0
    Echo Responses Received:                0
```

show services mobile-edge sessions

Syntax

```
show services mobile-edge sessions
<control-plane-peers | detail | extensive | summary>
show services mobile-edge sessions control-plane-peers
<address>
show services mobile-edge sessions detail
<control-plane-peers>
show services mobile-edge sessions extensive
<local-seid>
show services mobile-edge sessions summary
<access-network-peers | anchor-group | apns | control-plane-peers | pic | slot>
```

Release Information

Command introduced in Junos OS 19.4R1.

Description

This command gives information on mobile sessions active on the SAEGW-U.

> **NOTE:** The backup routing engine (RE) supports only the top level of the **show services mobile-edge sessions summary** command and not any of its sub-options.

Options

none—Display information on mobile sessions active on the SAEGW-U.

control-plane-peers—Display information on mobile sessions for a specific or all SAEGW-Cs.

detail—Display detailed information on mobile sessions or on a specific SAEGW-C.

extensive—Display extensive information on mobile sessions or by local SEID.

summary—Display summary information on mobile sessions active on the SAEGW-U.

access-network-peers—Display session summary output by access network peer.

anchor-group—Display session summary output by anchor group.

apns—Display session summary output by APN.

local-seid—Display session extensive output for a local SEID.

pic—Display session summary output by PIC.

slot—Display session summary output by FPC slot.

Required Privilege Level
view

RELATED DOCUMENTATION

Example: Configuring an MX Router as an SAEGW-U | 44

List of Sample Output

Output Fields

Table 9 on page 78 describes the output fields for the **show services mobile-edge sessions** command. Output fields are listed in the approximate order in which they appear.

Table 9: show services mobile-edge sessions Output Fields

Field Name	Field Description
Session-address	IP address of the session.
State	State of the session. ESTABLISHED or DELETING.
Num-bearers	Number of bearers for the session.
VRF-ID	The ID number (in hexadecimal format) of the routing-instance that the mobile-edge session's APN is attached to.
APN	Access Point Name
CPF-peer	IP address of the SAEGW-C peer for the session.

Table 9: show services mobile-edge sessions Output Fields *(continued)*

Field Name	Field Description
Access-peer	IP address of the access peer (eNodeB) for the session.
Anchor-PFE	Anchor PFE for the session.
Secondary-anchor-PFE	Backup anchor PFE for the session.
Local-SEID	Local session ID (SEID) for the session.
Remote-SEID	Remote SEID for the session.
Bearer EBI/NSAPI	EPS Bearer ID / Network Service Access Point Identifier.
Loc TEID	The local TEID allocated by the SAEGW-U for a given access peer.
Rem TEID	The remote TEID allocated for a given access peer. This is signaled over PFCP.
FAR-ID	Forwarding Action Rule ID.
Destination Interface	Destination Interface for a given FAR, either **Access** or **Core**.
PDR ID	Packet Detection Rule ID.
QER ID	QoS Enforcement Rule ID.
Uplink gate	Uplink QER gate status, either **Open** or **Closed**.
Downlink gate	Downlink QER gate status, either **Open** or **Closed**.
Uplink mbr	Uplink QER maximum bit rate before policing starts, in kbps.
Downlink mbr	Downlink QER maximum bit rate before policing starts, in kbps.
SDF Filter	Service data flow filter(s) for a given PDR. Flows matching these filters will be forwarded. All else are discarded.
Sessions by State	The current number of sessions in state: **ESTABLISHED**, **DELETING**, and **Total**.
Bearers by State	The current number of bearers in state: **BEARER_WAIT**, **ESTABLISHED**, **DELETING**, and **Total**.
APFE PIC	The anchor PFE PIC.

Table 9: show services mobile-edge sessions Output Fields *(continued)*

Field Name	Field Description
Slot	The FPC slot.

Sample Output

show services mobile-edge sessions

```
user@host> show services mobile-edge sessions
```

```
    Session-address: 23.0.21.163 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-3/0/0 Secondary-anchor-PFE: apfe0:pfe-2/0/0
        Local-SEID: 0x20015a2 Remote-SEID: 0x3cb2

    Session-address: 23.0.47.237 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-3/0/0 Secondary-anchor-PFE: apfe0:pfe-2/0/0
        Local-SEID: 0x2fec Remote-SEID: 0x56fc

    Session-address: 23.0.21.49 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-3/0/0 Secondary-anchor-PFE: apfe0:pfe-2/0/0
        Local-SEID: 0x1531 Remote-SEID: 0x3c40

    Session-address: 23.0.29.83 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-3/0/0 Secondary-anchor-PFE: apfe0:pfe-2/0/0
        Local-SEID: 0x2001d53 Remote-SEID: 0x4462

....
```

show services mobile-edge sessions control-plane-peers

```
user@host> show services mobile-edge sessions control-plane-peers
```

```
Peer Address: 20.3.1.3

    Session-address: 23.0.21.163 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-3/0/0 Secondary-anchor-PFE: apfe0:pfe-2/0/0
        Local-SEID: 0x20015a2 Remote-SEID: 0x3cb2

Peer Address: 20.3.1.3

    Session-address: 23.0.47.237 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-3/0/0 Secondary-anchor-PFE: apfe0:pfe-2/0/0
        Local-SEID: 0x2fec Remote-SEID: 0x56fc

Peer Address: 20.3.1.3

    Session-address: 23.0.21.49 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-3/0/0 Secondary-anchor-PFE: apfe0:pfe-2/0/0
        Local-SEID: 0x1531 Remote-SEID: 0x3c40

Peer Address: 20.3.1.3

    Session-address: 23.0.29.83 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6
        Anchor-PFE: apfe0:pfe-3/0/0 Secondary-anchor-PFE: apfe0:pfe-2/0/0
        Local-SEID: 0x2001d53 Remote-SEID: 0x4462

...
```

show services mobile-edge sessions detail

`user@host>` **show services mobile-edge sessions detail**

```
    Session-address: 87.0.28.184 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 30.71.1.3 Access-peer: 40.71.1.2
        Anchor-PFE: apfe0:pfe-4/0/0 Secondary-anchor-PFE: apfe0:pfe-1/0/0
        Local-SEID: 0x3001d6d Remote-SEID: 0x43c7
```

```
        Bearer EBI/NSAPI: 5 State: ESTABLISHED
            Loc TEID: 0x3072d0 Rem TEID: 0x6c7317

    Session-address: 87.0.33.234 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 30.71.1.3 Access-peer: 40.71.1.2
        Anchor-PFE: apfe0:pfe-4/0/0 Secondary-anchor-PFE: apfe0:pfe-1/0/0
        Local-SEID: 0x10021ea Remote-SEID: 0x48f9

        Bearer EBI/NSAPI: 5 State: ESTABLISHED
            Loc TEID: 0x1087a0 Rem TEID: 0x6c7849

    Session-address: 87.0.24.239 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 30.71.1.3 Access-peer: 40.71.1.2
        Anchor-PFE: apfe0:pfe-4/0/0 Secondary-anchor-PFE: apfe0:pfe-1/0/0
        Local-SEID: 0x20018ed Remote-SEID: 0x3ffe

        Bearer EBI/NSAPI: 5 State: ESTABLISHED
            Loc TEID: 0x2063b0 Rem TEID: 0x6c6f4e

    Session-address: 87.0.119.88 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 30.71.1.3 Access-peer: 40.71.1.2
        Anchor-PFE: apfe0:pfe-4/0/0 Secondary-anchor-PFE: apfe0:pfe-1/0/0
        Local-SEID: 0x300760d Remote-SEID: 0x9e67

        Bearer EBI/NSAPI: 5 State: ESTABLISHED
            Loc TEID: 0x70dd50 Rem TEID: 0x6ccdb7

...
```

show services mobile-edge sessions detail control-plane-peers

`user@host>` **show services mobile-edge sessions detail control-plane-peers *address***

```
Peer Address: 30.71.1.3
    Session-address: 87.0.28.184 State: ESTABLISHED Num-bearers: 1
        VRF-ID: 0x0 APN: default
        CPF-peer: 30.71.1.3 Access-peer: 40.71.1.2
        Anchor-PFE: apfe0:pfe-4/0/0 Secondary-anchor-PFE: apfe0:pfe-1/0/0
        Local-SEID: 0x3001d6d Remote-SEID: 0x43c7

        Bearer EBI/NSAPI: 5 State: ESTABLISHED
```

```
        Loc TEID: 0x3072d0 Rem TEID: 0x6c7317

Session-address: 87.0.33.234 State: ESTABLISHED Num-bearers: 1
    VRF-ID: 0x0 APN: default
    CPF-peer: 30.71.1.3 Access-peer: 40.71.1.2
    Anchor-PFE: apfe0:pfe-4/0/0 Secondary-anchor-PFE: apfe0:pfe-1/0/0
    Local-SEID: 0x10021ea Remote-SEID: 0x48f9

    Bearer EBI/NSAPI: 5 State: ESTABLISHED
        Loc TEID: 0x1087a0 Rem TEID: 0x6c7849

Session-address: 87.0.24.239 State: ESTABLISHED Num-bearers: 1
    VRF-ID: 0x0 APN: default
    CPF-peer: 30.71.1.3 Access-peer: 40.71.1.2
    Anchor-PFE: apfe0:pfe-4/0/0 Secondary-anchor-PFE: apfe0:pfe-1/0/0
    Local-SEID: 0x20018ed Remote-SEID: 0x3ffe

    Bearer EBI/NSAPI: 5 State: ESTABLISHED
        Loc TEID: 0x2063b0 Rem TEID: 0x6c6f4e
```

show services mobile-edge sessions extensive

`user@host>` **show services mobile-edge sessions extensive**

```
Session-address: 87.0.28.184 State: ESTABLISHED Num-bearers: 1
    VRF-ID: 0x0 APN: default
    CPF-peer: 30.71.1.3 Access-peer: 40.71.1.2
    Anchor-PFE: apfe0:pfe-4/0/0 Secondary-anchor-PFE: apfe0:pfe-1/0/0
    Local-SEID: 0x3001d6d Remote-SEID: 0x43c7

    Bearer EBI/NSAPI: 5 State: ESTABLISHED
        Loc TEID: 0x3072d0 Rem TEID: 0x6c7317

        FAR-ID: 1
        Destination Interface: Core

        FAR-ID: 2
        Destination Interface: Access

        PDR ID: 2

          QER ID: 1
            Uplink gate : Open      Downlink gate   : Open
            Uplink mbr  : 1000000000 kbps    Downlink mbr    : 1000000000 kbps
```

```
            SDF Filter:
              permit out ip from any to assigned

          PDR ID: 1

            QER ID: 1
              Uplink gate : Open      Downlink gate   : Open
             Uplink mbr  : 1000000000 kbps    Downlink mbr    : 1000000000 kbps

            SDF Filter:
              permit out ip from any to assigned

Session-address: 87.0.24.239 State: ESTABLISHED Num-bearers: 1
    VRF-ID: 0x0 APN: default
    CPF-peer: 30.71.1.3 Access-peer: 40.71.1.2
    Anchor-PFE: apfe0:pfe-4/0/0 Secondary-anchor-PFE: apfe0:pfe-1/0/0
    Local-SEID: 0x20018ed Remote-SEID: 0x3ffe

    Bearer EBI/NSAPI: 5 State: ESTABLISHED
        Loc TEID: 0x2063b0 Rem TEID: 0x6c6f4e

        FAR-ID: 1
        Destination Interface: Core

        FAR-ID: 2
        Destination Interface: Access

        PDR ID: 2

          QER ID: 1
            Uplink gate : Open      Downlink gate   : Open
           Uplink mbr  : 1000000000 kbps    Downlink mbr    : 1000000000 kbps

          SDF Filter:
            permit out ip from any to assigned

        PDR ID: 1

          QER ID: 1
            Uplink gate : Open      Downlink gate   : Open
           Uplink mbr  : 1000000000 kbps    Downlink mbr    : 1000000000 kbps

          SDF Filter:
```

```
                permit out ip from any to assigned

...
```

show services mobile-edge sessions summary

`user@host>` **show services mobile-edge sessions summary**

```
Sessions by State:
    SESSION_WAIT: 35
    ESTABLISHED: 18561
    Total: 18596

Bearers by State:
    BEARER_WAIT: 30
    ESTABLISHED: 18561
    Total: 18591
```

show services mobile-edge sessions summary access-network-peers

`user@host>` **show services mobile-edge sessions summary access-network-peers**

```
Summary by Access Peer:
Peer Address: 40.71.1.2
    Sessions by State:
    ESTABLISHED: 6426
    Total: 6426

    Bearers by State:
    ESTABLISHED: 6426
    DELETING: 4832
    Total: 11258
```

show services mobile-edge sessions summary anchor-group

`user@host>` **show services mobile-edge sessions summary anchor-group**

```
Summary by pic:
APFE PIC: apfe0:pfe-4/0
    Sessions by State:
    ESTABLISHED: 6421
    DELETING: 4832
```

```
    Total: 11253

    Bearers by State:
    BEARER_WAIT: 58696
    ESTABLISHED: 6421
    DELETING: 4927
    Total: 70044

Summary by pic:
APFE PIC: apfe0:pfe-1/0
    Sessions by State:
    ESTABLISHED: 6421
    DELETING: 4832
    Total: 11253

    Bearers by State:
    BEARER_WAIT: 58696
    ESTABLISHED: 6421
    DELETING: 4927
    Total: 70044
```

show services mobile-edge sessions summary apns

user@host> **show services mobile-edge sessions summary apns**

```
Summary by Access Point Names:
APN: default
    Sessions by State:
    ESTABLISHED: 6421
    DELETING: 4832
    Total: 11253

    Bearers by State:
    ESTABLISHED: 6421
    DELETING: 4832
    Total: 11253

Summary by Access Point Names:
APN: test.internet.488
    Sessions by State:
    Total: 0
```

```
    Bearers by State:
    Total: 0
```

show services mobile-edge sessions summary control-plane-peers

`user@host>` **show services mobile-edge sessions summary control-plane-peers**

```
Summary by Control Peer:
Peer Address: 30.71.1.3
    Sessions by State:
    ESTABLISHED: 6421
    DELETING: 4832
    Total: 11253

    Bearers by State:
    BEARER_WAIT: 58696
    ESTABLISHED: 6421
    DELETING: 4927
    Total: 70044
```

show services mobile-edge sessions summary pic

`user@host>` **show services mobile-edge sessions summary pic**

```
Summary by pic:
APFE PIC: pfe-1/0
    Sessions by State:
    ESTABLISHED: 6421
    DELETING: 4832
    Total: 11253

    Bearers by State:
    BEARER_WAIT: 58696
    ESTABLISHED: 6421
    DELETING: 4927
    Total: 70044

Summary by pic:
APFE PIC: pfe-4/0
    Sessions by State:
    ESTABLISHED: 6421
    DELETING: 4832
    Total: 11253
```

```
    Bearers by State:
    BEARER_WAIT: 58696
    ESTABLISHED: 6421
    DELETING: 4927
    Total: 70044
```

show services mobile-edge sessions summary slot

`user@host>` **show services mobile-edge sessions summary slot**

```
Summary by slot:
Slot: pfe-1
    Sessions by State:
    ESTABLISHED: 6421
    DELETING: 4832
    Total: 11253

    Bearers by State:
    BEARER_WAIT: 58696
    ESTABLISHED: 6421
    DELETING: 4927
    Total: 70044

Summary by slot:
Slot: pfe-4
    Sessions by State:
    ESTABLISHED: 6421
    DELETING: 4832
    Total: 11253

    Bearers by State:
    BEARER_WAIT: 58696
    ESTABLISHED: 6421
    DELETING: 4927
    Total: 70044
```

show services mobile-edge summary

Syntax

```
show services mobile-edge summary
```

Release Information

Command introduced in Junos OS 19.4R1.

Description

This command gives summary information on the SAEGW-U.

Required Privilege Level

view

RELATED DOCUMENTATION

Example: Configuring an MX Router as an SAEGW-U | 44

List of Sample Output

show services mobile-edge summary on page 90

Output Fields

Table 10 on page 89 describes the output fields for the **show services mobile-edge summary** command. Output fields are listed in the approximate order in which they appear.

Table 10: show services mobile-edge summary Output Fields

Field Name	Field Description
Graceful-Restart	Whether graceful-restart is enabled or disabled.
Mastership	Mastership state for the given routing engine (RE) this command is executed on. For the master RE, **Master** is displayed. For the backup RE, **Standby** is displayed. If GRES not enabled, **Standalone** is displayed.
State	State can be either **Running** or **Bulk Sync**. **Bulk Sync** implies we are waiting for synchronization.
Bulk Sync	Status of **Bulk Sync**. Must be **Synchronized** with GRES enabled to preserve state through daemon restart. Other states are **Synchronizing**or **N/A** (when GRES is not enabled).

Sample Output

show services mobile-edge summary

user@host> **show services mobile-edge summary**

```
Graceful-Restart        Enabled
Mastership              Master
State                   Running
Bulk Sync               Synchronized
```