

Junos Multi-Access User Plane User Guide

Published
2021-12-14

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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

Junos Multi-Access User Plane User Guide
Copyright © 2021 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <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 This Guide | v

1

Understanding Junos Multi-Access User Plane

Junos Multi-Access User Plane Overview | 2

Introduction | 2

3GPP TS 29.244 Release 15 Support | 11

Hardware and Software Requirements | 12

CUPS Session Creation and Data Flow with Junos Multi-Access User Plane | 13

CUPS Session Creation | 14

CUPS Session Data Flow | 17

Charging and Usage Reports | 18

Handover between eNodeBs and no SGW or SAEGW Change | 19

Handover with SGW Change | 21

GRES on Junos Multi-Access User Plane | 23

2

Configuring Junos Multi-Access User Plane

MX Series Router As Junos Multi-Access User Plane | 31

Overview | 31

Configuring Junos Multi-Access User Plane on an MX Router | 35

DDoS Attack Protection Configuration | 36

GRES Configuration | 36

Chassis Configuration for the Anchor PFE Line Cards | 37

Interface Configuration | 37

Mobile Edge Configuration | 39

Anchor PFEs and Redundancy in Junos Multi-Access User Plane | 41

Understanding the Anchor PFE | 41

Configuring No Redundancy for the Anchor PFEs | 41

| [Configuring 1:1 Hot-standby Redundancy for the Anchor PFEs](#) | 42

Example: Configuring an MX Router as an SAEGW-U | 45

| [Requirements](#) | 45

| [Overview](#) | 47

| [Configuration](#) | 48

| [Verification](#) | 55

3

Configuration Statements

[apn-services \(control plane services\)](#) | 61

[forwarding-packages](#) | 62

[mobility](#) | 64

[peer-groups \(access network peers\)](#) | 66

[peer-groups \(control plane peers\)](#) | 68

[peer-groups \(core network peers\)](#) | 70

[saegw](#) | 72

[saegw access-network-peers](#) | 74

[saegw control-plane-peers](#) | 76

[saegw-core-network-peers](#) | 79

[saegw system](#) | 82

4

Operational Commands

[show services mobile-edge peers](#) | 85

[show services mobile-edge sessions](#) | 89

[show services mobile-edge summary](#) | 104

About This Guide

Use this guide to understand the Junos Multi-Access User Plane and how to configure an MX Series router as an SAEGW-U, SGW-U, PGW-U, and UPF to provide high-throughput 4G and 5G mobility and fixed wireless services.

1

CHAPTER

Understanding Junos Multi-Access User Plane

Junos Multi-Access User Plane Overview | 2

CUPS Session Creation and Data Flow with Junos Multi-Access User Plane | 13

GRES on Junos Multi-Access User Plane | 23

Junos Multi-Access User Plane Overview

IN THIS SECTION

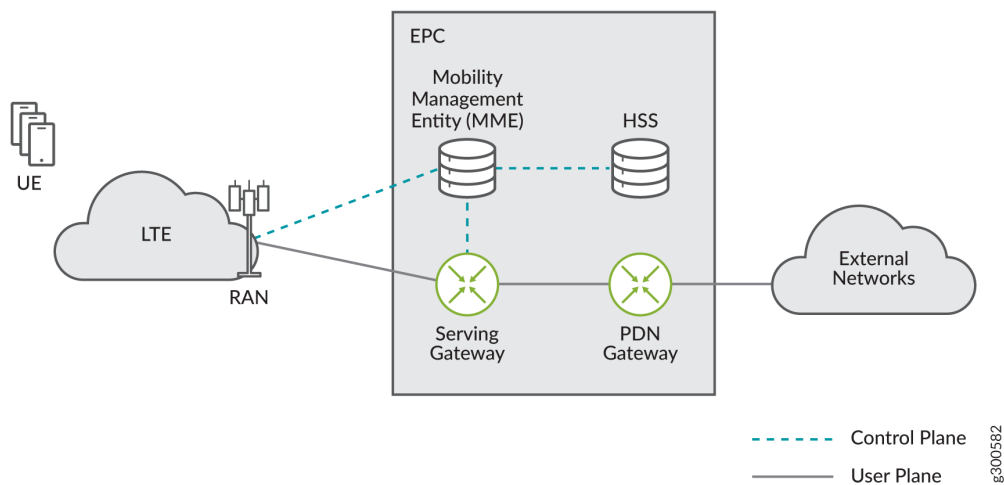
- Introduction | 2
- 3GPP TS 29.244 Release 15 Support | 11
- Hardware and Software Requirements | 12

Introduction

The 3rd Generation Partnership Project (3GPP) introduced the Evolved Packet Core (EPC) for core network architecture. As [Figure 1 on page 2](#) shows, the four main EPC network elements are:

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

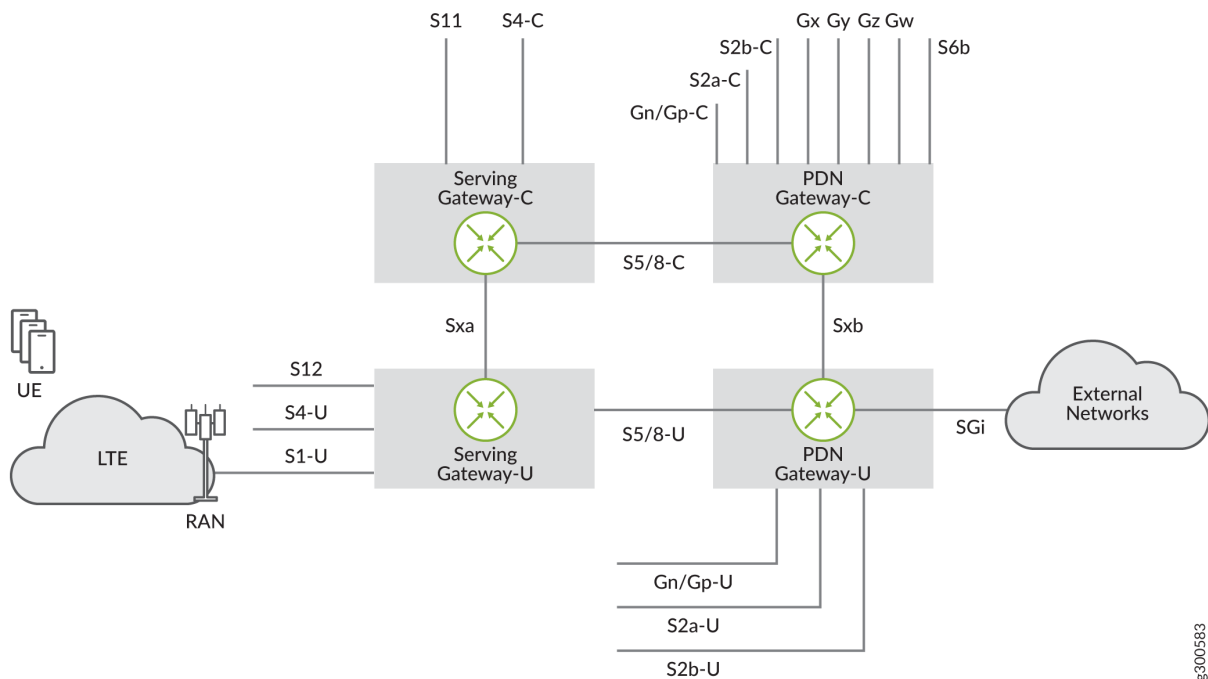
Figure 1: 3GPP Evolved Packet Core Architecture



User Equipment (UE) has control path connectivity 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 TS 29.244 Release 14 introduced CUPS, which stands for Control and User Plane Separation. CUPS provides the architecture enhancements for the separation of functionality in the EPC's serving gateway (SGW) and PDN gateway (PGW). As [Figure 2 on page 3](#) shows, both the SGW and the PGW 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

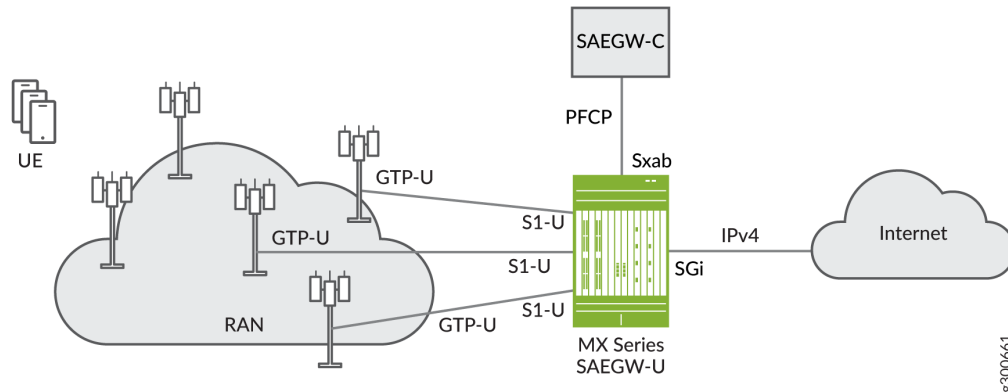
With this functional separation, the control plane and the user plane have very distinct deployment requirements and can be in different physical locations. While the control plane function is very complex, the user plane function requires high packet processing capability and rich policy enforcement. You can distribute the user plane more than the control plane and locate the user plane closer to end-user access points. This distribution enables higher bandwidth per user while delivering lower latency. Control plane and user plane separation provides the following benefits:

- Independent scaling of the user plane and the control plane
- 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.

Junos Multi-Access User Plane supports a combined SGW user plane (SGW-U) and PGW user plane (PGW-U) in a single MX series router (see [Figure 3 on page 5](#)). 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, referred to as a SAEGW-C, through a combined Sxab interface.

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

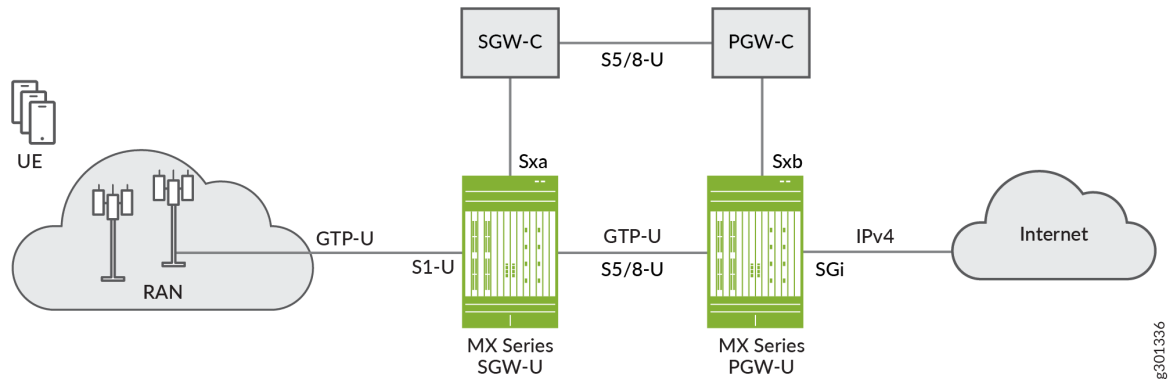
Figure 3: Junos Multi- Access User Plane SAEGW-U



Junos Multi-Access User Plane also supports running an MX router as either a standalone SGW-U or a standalone PGW-U. A standalone SGW-U enables high-throughput 4G **mobility service** (relocation of a UE to a new eNodeB, new SGW-U, or new SAEGW-U). Junos Multi-Access User Plane support GTP-U based S5-U and S8-U interfaces, which are links between SGW-U and PGW-U devices. Junos Multi-Access User Plane also provides tunnel relay functionality to forward user plane traffic between S1-U and S5-U/S8-U interfaces and between S5-U/S8-U and SGi interfaces.

Figure 4 on page 6 shows the basic topology of running MX routers separately as and SGW-U and a PGW-U to enable mobility.

Figure 4: Junos Multi-Access User Plane SGW-U and PGW-U



SGW-Cs and PGW-Cs handle logistics of UE handover, including SGW & PGW selection. The SGW-C and PGW-C participate in control protocol exchanges and update their SGW-U/PGW-U counterparts with any new or changed attributes of the UE session and bearers.

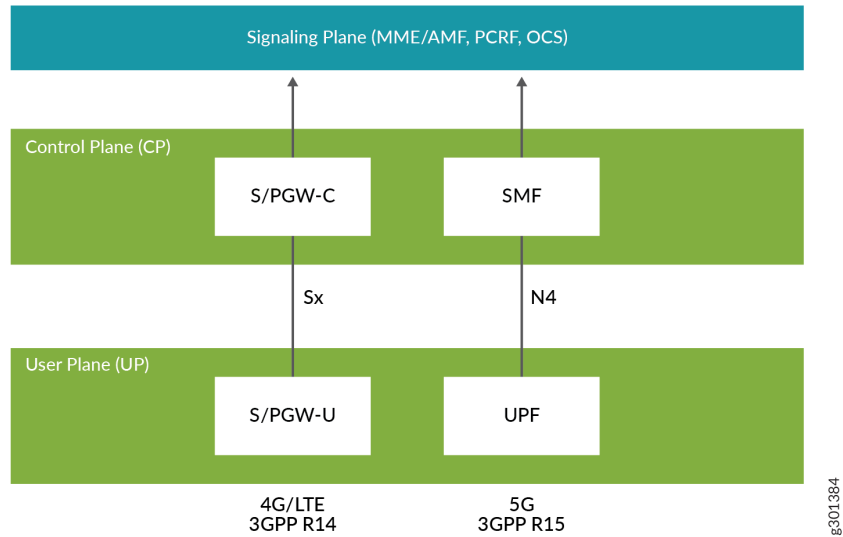
We support the following mobility scenarios:

- Handover with eNodeB and no SGW change
- Handover with SGW change (direct forwarding)
- Handover with SGW change (indirect forwarding)

Junos Multi-Access User Plane supports 5G user plane function (UPF) in addition to the SAEGW-U/SGW-U/PGW-U functions (see Figure 5 on page 7). Junos Multi-Access User Plane supports seamless transition from 4G to 5G services by supporting both networks on the same MX Series router with the

same configuration. Junos Multi-Access User Plane supports 4G sessions and 5G sessions simultaneously.

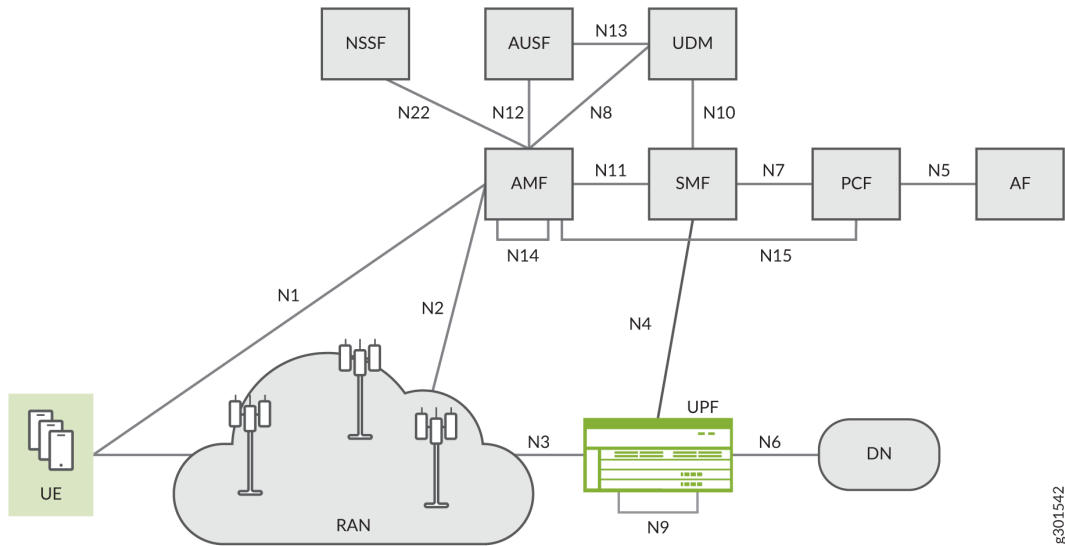
Figure 5: Support for both 4G/LTE and 5G User Plane Functionality



Junos Multi-Access User Plane supports MX routers functioning as user plane functions (UPFs) in accordance with 3GPP Release 15 CUPS architecture. The UPF provides high-throughput 5G fixed wireless and mobile wireless service in non-standalone (NSA) mode.

Figure 6 on page 8 shows the basic topology of running an MX router as a UPF to enable 5G services.

Figure 6: Junos Multi-Access UPF in 5G CUPS Architecture



The 5G system architecture consists of the following network functions:

- Authentication Server Function (AUSF)
- Access and Mobility Management Function (AMF)
- Data Network (DN), e.g. operator services, Internet access or 3rd party services
- Network Slice Selection Function (NSSF)
- Policy Control Function (PCF)
- Session Management Function (SMF)
- Unified Data Management (UDM)
- User Plane Function (UPF)
- Application Function (AF)
- User Equipment (UE)
- (Radio) Access Network ((R)AN)

The session management function (SMF) includes the following functionality. A single instance of an SMF can support some or all of the SMF functionalities.

- Session management, e.g. session establishment, modify and release, including tunnel maintain between the UPF and a RAN node
- UE IP address allocation and management (including optional authorization)
- DHCPv4 (server and client) and DHCPv6 (server and client) functions
- Selection and control of the UPF
- Configure traffic steering at the UPF to route traffic to the proper destination
- Termination of interfaces towards policy control functions
- Charging data collection and support of charging interfaces
- Control and coordination of charging data collection at UPF
- Termination of SM parts of NAS messages
- Downlink data notification
- Initiator of RAN-specific SM information, sent via AMF over N2 to AN
- Determine SSC mode of a session
- Roaming functionality:
 - Handle local enforcement to apply QoS SLAs (VPLMN)
 - Charging data collection and charging interface (VPLMN)
 - Support for interaction with external DN for transport of signaling for PDU session authentication/authorization by external DN

The user plane function (UPF) includes the following functionality. A single instance of a UPF can support some or all of the UPF functionalities.

- Anchor point for Intra-/Inter-RAT mobility (when applicable)
- External PDU session point of interconnect to the data network
- Packet routing and forwarding
- Packet inspection
- User plane part of policy rule enforcement, e.g., gating, redirection, traffic steering)
- Traffic usage reporting

- QoS handling for user plane, e.g. uplink/downlink rate enforcement, reflective QoS marking in the downlink direction
- Uplink traffic verification (SDF to QoS Flow mapping)
- Transport level packet marking in the uplink and the downlink directions
- Downlink packet buffering and downlink data notification triggering
- Sending and forwarding of one or more end marker messages to the source RAN node

Junos Multi-Access User Plane acts as the UPF in the 5G CUPs architecture and includes support for the following:

- N3, N4, N6, and N9 interface support
- Roaming through the N9 interface
- GPRS tunneling protocol, user plane (GTP-U) tunneling to the control plane
- QoS Flow ID (QFI) support for 5G QoS flows

N3, N4, and N6 interfaces are similar to S1-U, Sx, and SGi interfaces in the 4G CUPs architecture, respectively. The N9 interface is similar to the S5/8-U interface. The N9 interface carries GTP-U encapsulated traffic and only connects from one UPF to another. In home-routed roaming scenarios, N9 reference points carry the user plane traffic back to an anchor UPF in the Home Public Land Mobile Network (HPLMN). Junos Multi-Access User Plane supports either a single N9 reference point or a single N6 reference point per PDU session.

QoS in 4G networks is bearer-based where the mapping is one to one between a bearer and a radio bearer. QoS in 5G networks is flow-based where a QFI (QoS Flow Identifier) classifies and marks packets. Multiple QoS flows map to a radio bearer. Each QoS flow is associated with two parameters, a 5G QoS Identifier (5QI) and an allocation and retention priority (ARP).

In summary, starting with Junos OS Release 21.2R1, Junos Multi-Access User Plane supports four different modes of operation on a single MX router:

- **SGW-U**, where the MX router acts as an SGW-U for all sessions and connects to a third-party SGW-C over a single Sxa interface and Juniper or third party PGW-Us over multiple S5/8-U interfaces.
- **PGW-U**, where the MX router acts as a PGW-U for all sessions and connects to a third-party PGW-C over a single Sxb interface and Juniper or third-party SGW-Us over multiple S5/8-U interfaces.
- **Combined SGW/PGW-U (SAEGW-U)**, where depending on the UE location, the MX router acts as an SGW-U for some sessions, a PGW-U for another set of sessions and SAEGW-U for the remaining sessions. In this mode, the SAEGW-U connects to an SAEGW-C over a single Sxab interface and to other Juniper or third-party SGW-Us and PGW-Us over multiple S5/8-U interfaces.

- **UPF**, where the MX router acts as a UPF for all sessions and connects to a third-party SMF over a single N4 interface and to other Juniper or third-party UPFs over multiple N9 interfaces.

3GPP TS 29.244 Release 15 Support

Junos Multi-Access User Plane supports elements of 3GPP TS 29.244 Release 15, including support for the following functionality:

- **PDI Optimization Support**—Packet Detection Information (PDI) optimization is an optional feature that enables the control plane function (CPF) to optimize the signaling towards the UPF by combining the information that is common to multiple Packet Detection Rules (PDRs) as a Traffic Endpoint with a Traffic Endpoint ID (TEID) and then referring to this Traffic Endpoint in messaging. The Traffic Endpoint ID is unique within a PFCP session.
- **GTP Path Management**—GTP path management provides heartbeat and error indication over GTP-U interfaces. A GTP-U peer can send an echo request on a path to a GTP-U peer to find out if it is alive. Junos Multi-Access User Plane devices support responding to echo requests.
- **User ID Support**—The user ID is an information element (IE) that can be present in a PFCP Session Establishment Request. This IE is useful for troubleshooting problems in the UPF affecting a subscriber. The IE is visible in the output for the `show services mobile-edge sessions` extensive command. The user ID is an optional, noncritical IE that can be any length up to 16 digits or 8 characters.
- **Transport Level Marking**—For EPC, the SGW and PGW perform transport level marking on a per EPS bearer basis. Transport level marking is the process of marking traffic with a DSCP value based on the locally configured mapping from the QCI and optionally the ARP level. The CPF can change the transport level marking by changing the Transport Level Marking IE in the related Forwarding Action Rule (FAR).

NOTE: Juniper Multi-Access User Plane supports transport level marking per bearer for downlink data only.

Transport Level Marking—For 5GC (5G core), transport level marking occurs on a per QoS flow basis. Transport level marking is the process of marking traffic at the UPF with a DSCP value based on the mapping from the 5QI, the priority level (if explicitly signaled) and, optionally, the ARP priority level configured at the SMF.

- **DDoS Support**—DDoS support is provided for PFCP and GTP path management. To configure DDoS for these protocols, see *protocols (DDoS)*.

- **QoS control/enforcement at the bearer level**—For QoS control/enforcement at the bearer level, the CPF must create the necessary PRDs to represent the service data flow, bearer, or session. The CPF must also create QERs for the QoS enforcement of the aggregate of the SDFs with the same bearer.

Junos Multi-Access User Plane supports QoS enforcement at either the service data flow (SDF) or the bearer level. If the MX router as UPF receives more than one QER for a bearer, it enforces QoS at the SDF level. If the MX router as UPF receives one QER for a bearer, it enforces QoS at the bearer level.

Hardware and Software Requirements

This section lists the MX Series hardware and software requirements needed to implement Junos Multi-Access User Plane.

[Table 1 on page 12](#) describes the hardware and software requirements for the Junos Multi-Access User Plane solution.

Table 1: Junos Multi-Access User Plane Platform Support

Junos OS Release	Supported Platforms	Line Cards Supporting Anchor PFE Interfaces	Line Cards Supporting Signaling, Ingress, and Egress Interfaces	Supported Routing Engines
Starting in Junos OS Release 19.4R1	<ul style="list-style-type: none"> • MX240 • MX480 • MX960 	<ul style="list-style-type: none"> • MPC7 	<ul style="list-style-type: none"> • MPC2 • MPC3 • MPC4 • MPC5 • MPC7 	<ul style="list-style-type: none"> • RE-S-1800X4-32G-S • RE-S-X6-64G-S • RE-S-X6-128G
Starting in Junos OS Release 20.2R1	<ul style="list-style-type: none"> • MX204 • MX10003 	<ul style="list-style-type: none"> • MX10003-LC2103 	<ul style="list-style-type: none"> • MX10003-LC2103 	

Table 1: Junos Multi-Access User Plane Platform Support *(Continued)*

Junos OS Release	Supported Platforms	Line Cards Supporting Anchor PFE Interfaces	Line Cards Supporting Signaling, Ingress, and Egress Interfaces	Supported Routing Engines
------------------	---------------------	---	---	---------------------------

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

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

Release History Table

Release	Description
21.3R1	Starting in Junos OS Release 21.3R1, Junos Multi-Access User Plane provides a long-route implementation as a replacement for a filter-based implementation to steer traffic to the anchor Packet Forwarding Engine removing the need for a firewall filter to route GTP packets.
21.2R1	Starting in Junos OS Release 21.2R1, Junos Multi-Access User Plane supports routers functioning as user plane functions (UPFs) in accordance with 3GPP Release 15 CUPS architecture.
20.4R1	Starting with Junos OS Release 20.4R1, Junos Multi-Access User Plane supports running an MX router as either a standalone SGW-U or a standalone PGW-U.
20.4R1	Starting with Junos OS Release 20.4R1, Junos Multi-Access User Plane supports elements of 3GPP TS 29.244 Release 15.

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

IN THIS SECTION

- [CUPS Session Creation | 14](#)
- [CUPS Session Data Flow | 17](#)
- [Charging and Usage Reports | 18](#)

- Handover between eNodeBs and no SGW or SAEGW Change | 19
- Handover with SGW Change | 21

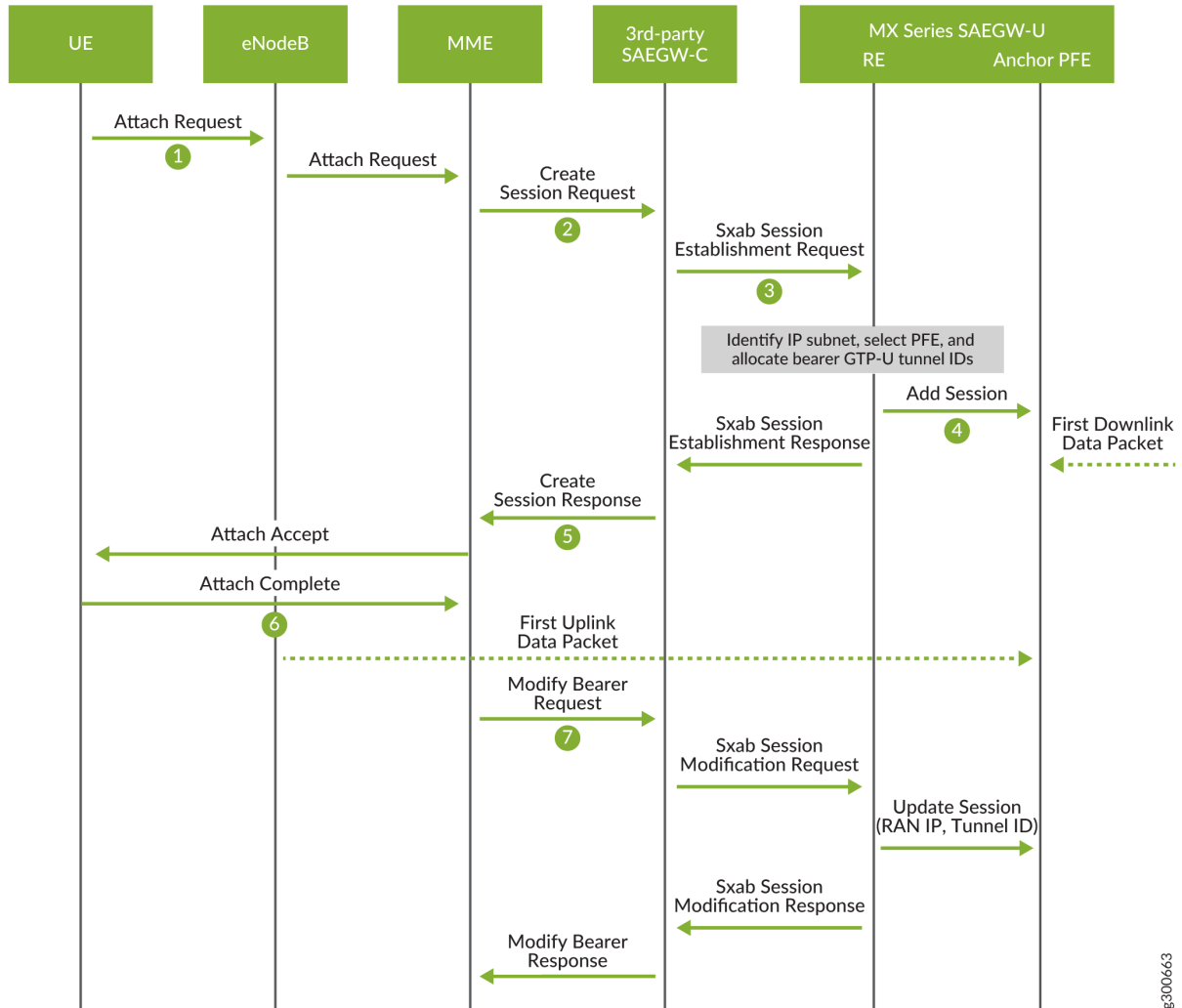
With the introduction of CUPS, it's useful to illustrate how an end-user session is created, how data flows during the session, and how the session is terminated with Junos Multi-Access User Plane.

CUPS Session Creation

NOTE: Before a CUPS session can be created, the control plane function (SAEGW-C, SGW-C, PGW-C) must create an Sx association with the user plane function (SAEGW-U, SGW-U, PGW-U). The control plane sends an Sx Association Setup Request message and the user plane responds with an Sx Association Setup Response message to create the association. Once this is done, the control plane can create Sx sessions on the user plane.

When an end user wants to access the network, a CUPS session must be created. [Figure 7 on page 15](#) illustrates this process once an Sx association is established between an SAEGW-C and an SAEGW-U.

Figure 7: CUPS Session Creation for SAEGW-C and SAEGW-U



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 Sxab 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 Sxab 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 Sxab 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

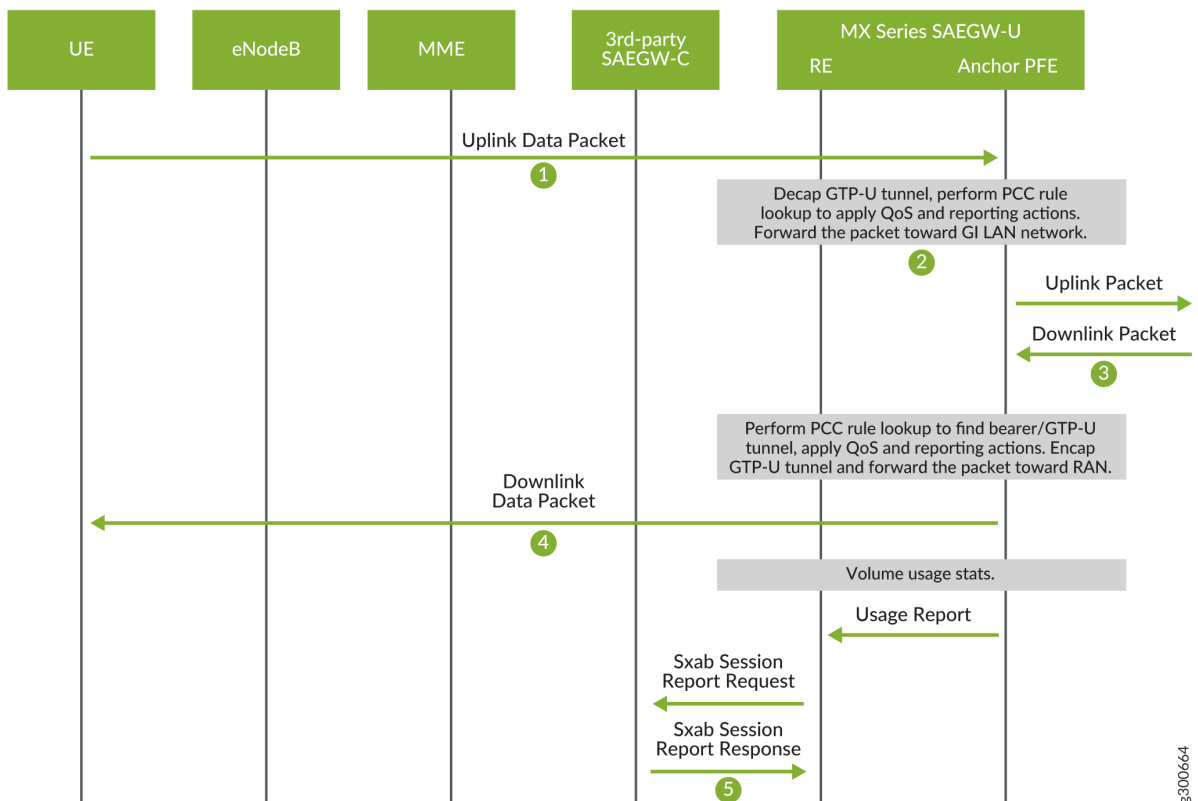
Junos Multi-Access User Plane does not support Buffering Action Rules (BARs).

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 8 on page 17](#).

Figure 8: 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 by way of the S1-U interface.
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 packet to the core network over the SGi interface.
3. The SAEGW-U receives a downlink IPv4 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 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 Sx 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). Rating groups can be created per session data flow (SDF) or for an entire bearer consisting of many SDFs.
2. The SAEGW-C associates a Usage Reporting Rule (URR) ID with a PDR and sends the 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.

NOTE: The SAEGW-U supports pausing charging measurements for any URR ID where the SAEGW-C sets the Inactive Measurement flag of the Measurement Information IE of the URR. The SAEGW-U also supports sending immediate reports to the SAEGW-C on a URR

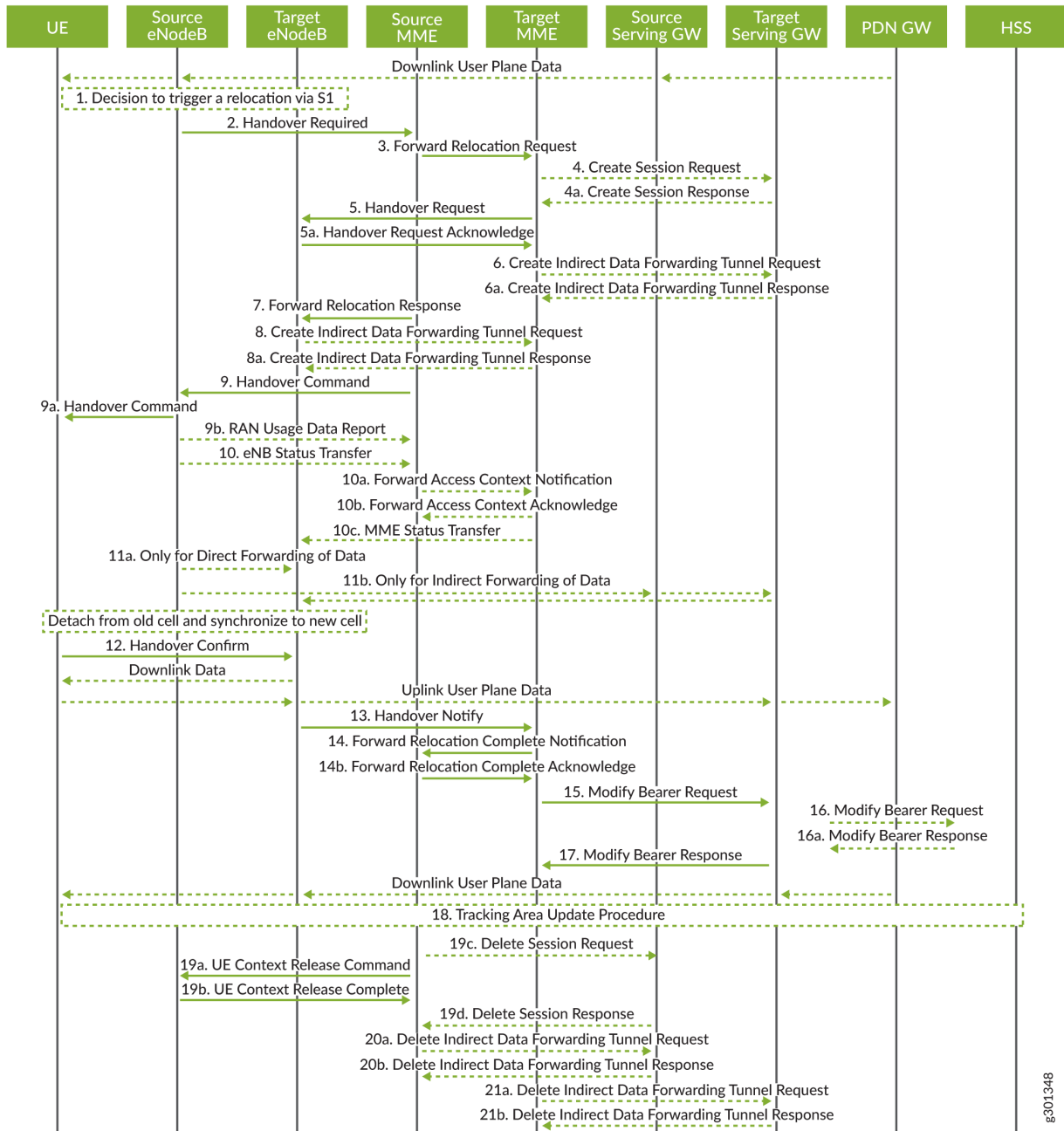
query or remove request from the SAEGW-C; the SAEGW-U sends the usage report in the Modify Response.

Handover between eNodeBs and no SGW or SAEGW Change

Starting with Junos OS 20.4R1, Junos Multi Access User Plane supports UE mobility.

Figure 9 on page 20 shows the entire handover process when a UE switches from one eNodeB to another without requiring a SGW or SAEGW change (i.e., both eNodeBs are served by the same SGW). This is the simplest version of mobility handover.

Figure 9: Handover between eNodeBs



The following steps describe just the interactions between the control plane and user plane functions of the SGW and PGW (steps 15-17 in Figure 9 on page 20).

Step 15: Target MME to Target SGW Modify Bearer Request

1. SGW-C sends Sx Session Modification Request to MX SGW-U. The message includes F-TEIDu(s) corresponding to the new eNodeB. It may also instruct MX SGW-U to send “end marker” message towards the new eNodeB.
2. If requested to do so, MX SGW-U sends “end marker” message on S1-U interface towards the old eNodeB for all bearers referred to by Sx Session Modification Message.
3. MX SGW-U updates downlink peer F-TEID in the bearer(s) to F-TEIDu(s) received in the Sx Session Modification Request.
4. MX SGW-U sends Sx Session Modification Response to SGW-C

Step 16: Target SGW to PGW Modify Bearer Request

NOTE: This step doesn't affect any F-TEIDu assignments on any of the bearers. It may however update other forwarding & charging parameters based on the new location of the UE.

1. PGW-C sends Sx Session Modification Request to MX PGW-U.
2. MX PGW-U updates corresponding bearers and sends Sx Session Modification Response to PGW-C.

Handover with SGW Change

Considering the CUPS model, there are two types of procedures involving SGW change:

- **Type 1:** Only Create Session Request message is sent from MME/SGSN to SGW-C during SGW change.
- **Type 2:** Create Session Request message followed by Modify Bearer Request message is sent from MME/SGSN to SGW-C during SGW change.

For the MX SGW-U, the main difference between these two types is that in the first, the new SGW-C is provided with both eNodeB and PGW F-TEIDu(s) within Create Session Request, while in the second, the eNodeB's F-TEIDu(s) are provided in the Modify Bearer Request, which translates to one extra Sx Session Modify Request/Response exchange between SGW-C and SGW-U. Because Type 1 can be considered a subset of Type 2, we present here the process for Type 2 handover.

[Figure 9 on page 20](#) shows the entire handover process when a UE switches from one eNodeB to another with requiring a SGW change. The following steps describe just the interactions between the control plane and user plane functions of the SGW and PGW (steps 4,4a, 15-17 and 19 in [Figure 9 on page 20](#)).

Step 4: Target MME to Target SGW Create Session Request

1. The target SGW-C sends Sx Session Establishment Request to the target MX SGW-U. If PGW-U is a different physical node than the target SGW-U, the message includes F-TEIDu(s) of the PGW-U for every bearer of the session. It does not include local F-TEIDu(s) since MX SGW-U only supports UP function allocated local F-TEIDu.
2. The target MX SGW-U creates a new session and allocates local F-TEIDu(s) for all bearers indicated in Sx Session Establishment Request. If the message included PGW-U's F-TEIDs, we use them to set uplink peer F-TEIDu(s) for all referenced bearers.
3. The target MX SGW-U sends Sx Session Establishment Response message to the target SGW-C.

Step 15: Target MME to Target SGW Modify Bearer Request

1. The target SGW-C sends Sx Session Modification Request to the target MX SGW-U. The message includes F-TEIDu(s) for all bearers corresponding to the new eNodeB.
2. The target MX SGW-U updates downlink peer F-TEID in the bearer(s) to F-TEIDu(s) received in the Sx Session Modification Request.
3. MX SGW-U sends Sx Session Modification Response to SGW-C.

Step 16: Target SGW to PGW Modify Bearer Request

1. PGW-C sends Sx Session Modification Request to MX PGW-U. The message includes F-TEIDu(s) of the target SGW-U for all bearers. It may also instruct MX PGW-U to send "end marker" message.
2. If instructed to do so, MX PGW-U sends "end marker" message towards old SGW-U.
3. MX PGW-U updates downlink peer F-TEID for all the referenced bearers to F-TEIDu(s) received in the Sx Modification Request Message
4. MX PGW-U sends Sx Session Modification Response to the target SGW-C.

Step 19: Source MME to Source SGW Delete Session Request

1. Source SGW-C sends Sx Session Delete Request to the source MX SGW-U.
2. Source MX SGW-U deletes all bearers and the session.
3. Source MX SGW-U sends Sx Session Delete Response to the source SGW-C.

Release History Table

Release	Description
20.4R1	Starting with Junos OS 20.4R1, Junos Multi Access User Plane supports UE mobility.

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 primary Routing Engine starts answering peer keepalives.

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

Primary Role switches to the backup Routing Engine if:

- The primary Routing Engine kernel stops operating.
- The primary 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 primary Routing Engine after 2 seconds, it determines that the primary Routing Engine has failed; and assumes primary role.

The Packet Forwarding Engine:

- Seamlessly disconnects from the old primary Routing Engine
- Reconnects to the new primary Routing Engine
- Does not reboot

- Does not interrupt traffic

The new primary Routing Engine and the Packet Forwarding Engine then become synchronized. If the new primary 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.

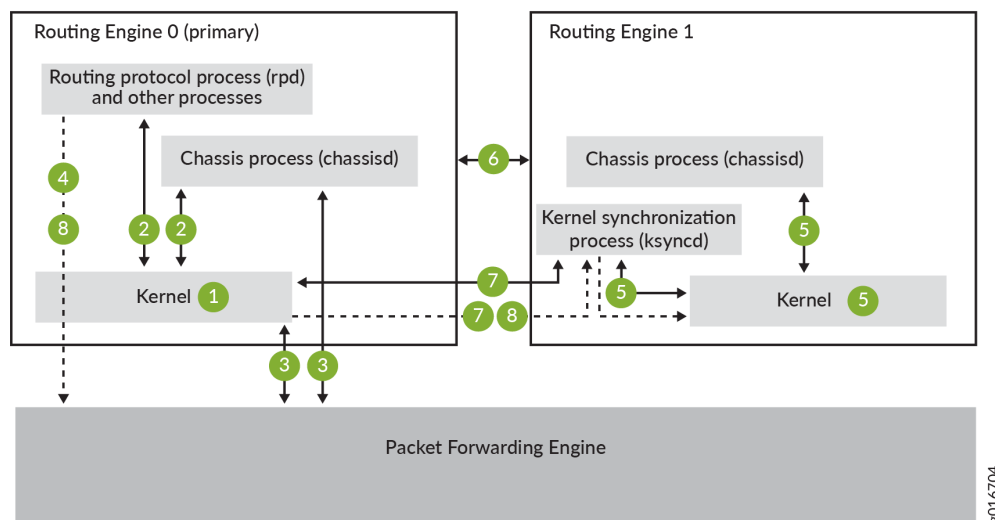
If the router or switch displays a warning message similar to Standby Routing Engine is not ready for graceful switchover. Packet Forwarding Engines that are not ready for graceful switchover might be reset, do not attempt switchover. If you choose to proceed with switchover, only the Packet Forwarding 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 10 on page 25 shows the system architecture of graceful Routing Engine switchover and the process a routing platform follows to prepare for a switchover.

Figure 10: 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 primary Routing Engine
- The show system switchover command from the Backup Routing Engine

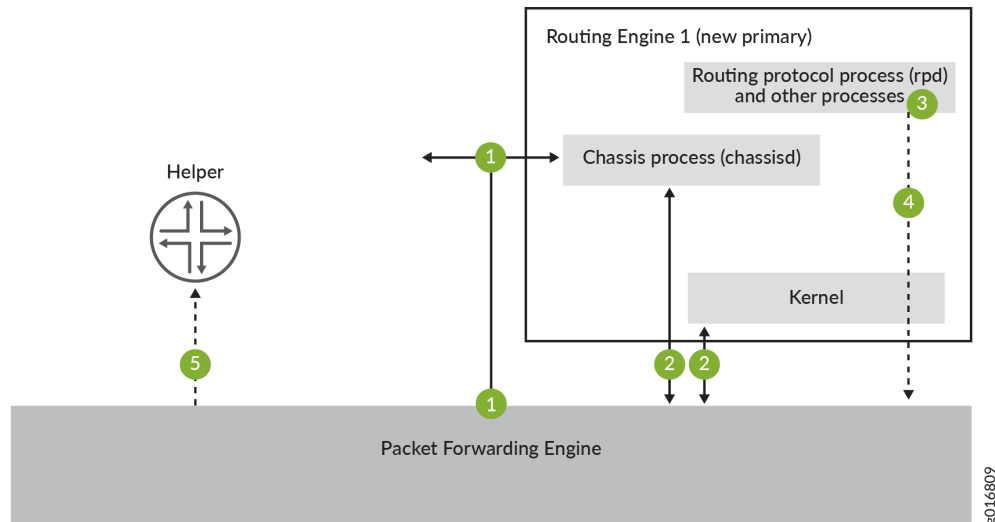
The switchover preparation process for GRES is as follows:

1. The primary 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 primary 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 primary Routing Engine.

8. After ksyncd completes the synchronization, all state information and the forwarding table are updated.

Figure 11 on page 26 shows the effects of a switchover on the routing (or switching)platform.

Figure 11: Graceful Routing Engine Switchover Process



A switchover process consists of the following steps:

1. When keepalives from the primary 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 primary.
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 primary 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 primary 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 2: Effects of a Routing Engine Switchover

Feature	Benefits	Considerations
Dual Routing Engines only (no features enabled)	<ul style="list-style-type: none"> When the switchover to the new primary Routing Engine is complete, routing convergence takes place and traffic is resumed. 	<ul style="list-style-type: none"> 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 primary Routing Engine. The switchover takes several minutes. All of the router's adjacencies are aware of the physical (interface alarms) and routing (topology) changes.

Table 2: Effects of a Routing Engine Switchover (*Continued*)

Feature	Benefits	Considerations
GRES enabled	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> The new primary 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 <i>and</i> NSR enabled	<ul style="list-style-type: none"> Traffic is not interrupted during the switchover. Interface, mobile-edge subscriber information, and kernel information are preserved. 	<ul style="list-style-type: none"> 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 2: Effects of a Routing Engine Switchover (*Continued*)

Feature	Benefits	Considerations
GRES and graceful restart enabled	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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](#)

2

CHAPTER

Configuring Junos Multi-Access User Plane

[MX Series Router As Junos Multi-Access User Plane | 31](#)

[Anchor PFEs and Redundancy in Junos Multi-Access User Plane | 41](#)

[Example: Configuring an MX Router as an SAEGW-U | 45](#)

MX Series Router As Junos Multi-Access User Plane

IN THIS SECTION

- [Overview | 31](#)
- [Configuring Junos Multi-Access User Plane on an MX Router | 35](#)

Overview

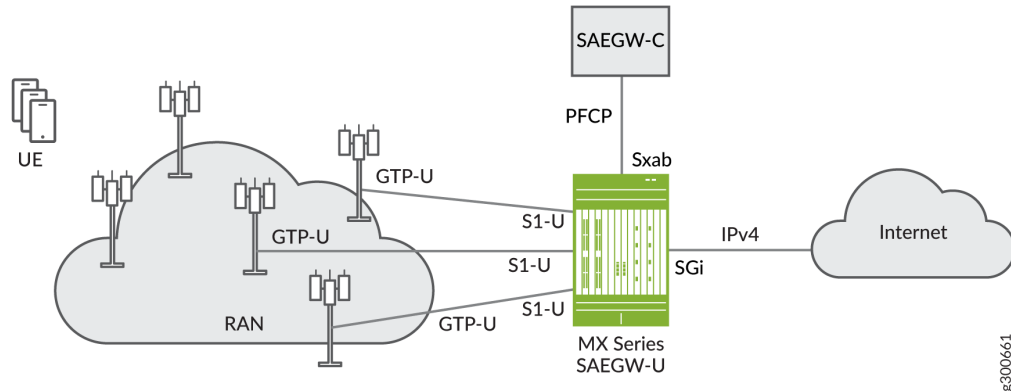
Junos Multi-Access User Plane on a single MX Series router can function in four modes:

- As 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). The SAEGW-U interoperates with a third-party SAEGW-C through a combined Sxab interface.
- As a standalone SGW user plane (SGW-U). The SGW-U interoperates with a third-party SGW-C through a the Sxa interface and one or more Juniper or third-party PGW-Us over one or more S5/8-U interfaces.
- As a standalone PGW user plane (PGW-U) in a single MX router. The PGW-U interoperates with a third-party PGW-C through a the Sxb interface and one or more Juniper or third-party SGW-Us over one or more S5/8-U interfaces.
- As a standalone user plane function (UPF) for carrying 5G traffic. The UPF interoperates with a third-party session management function (SMF).

Configuring Junos Multi-Access User Plane on an MX Series router is essentially the same for each of these functions. This topic describes this configuration process.

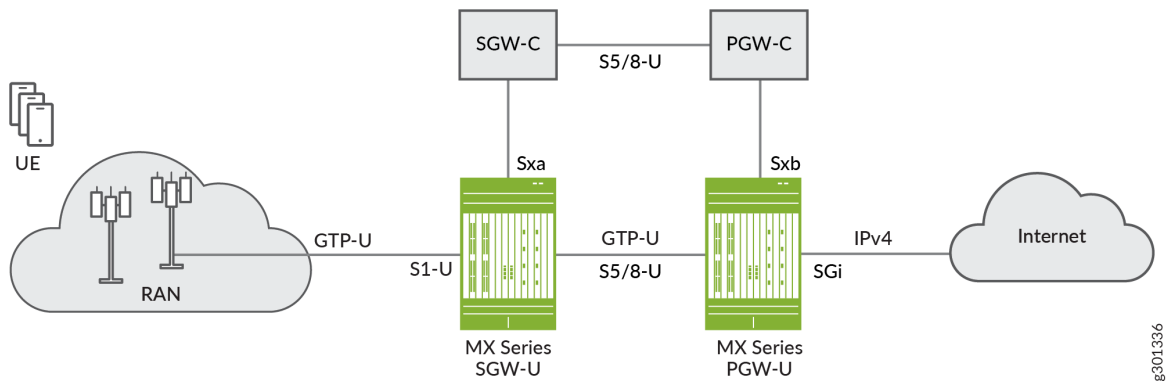
As [Figure 12 on page 32](#) shows, Juniper's MX SAEGW-U interoperates with a third-party SAEGW-C through a combined Sxab interface.

Figure 12: MX Series SAEGW-U in the CUPS Wireless Network Architecture



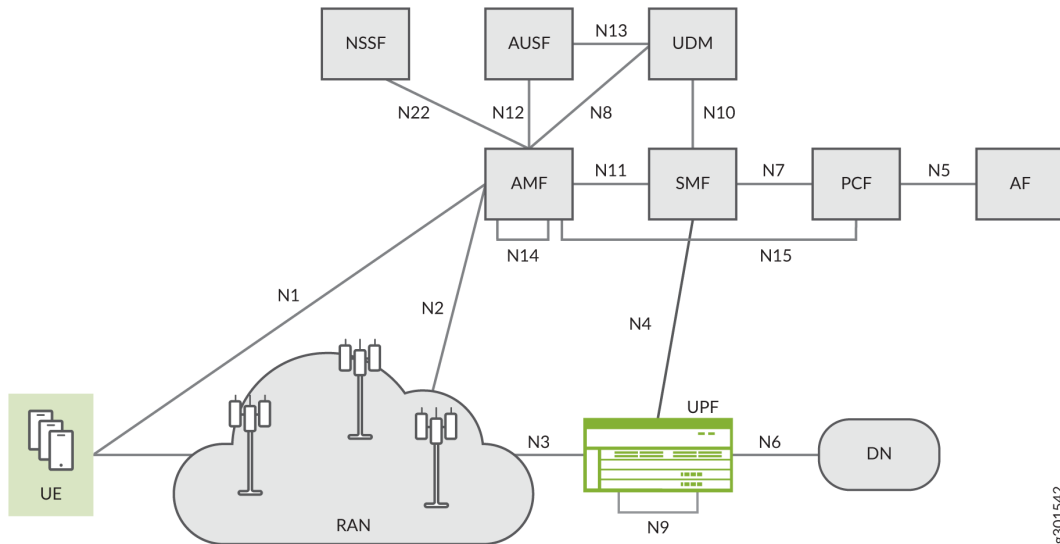
As [Figure 13 on page 32](#) shows, the SGW-U interoperates with a third-party SGW-C through a the Sxa interface and one or more Juniper or third-party PGW-Us over one or more S5/8-U interfaces. The PGW-U interoperates with a third-party PGW-C through a the Sxb interface and one or more Juniper or third-party SGW-Us over one or more S5/8-U interfaces.

Figure 13: MX Series SGW-U and PGW-U in the CUPS Wireless Network Architecture



As [Figure 14 on page 33](#) shows, Juniper's MX UPF interoperates with a third-party SMF through the N4 interface.

Figure 14: MX Series UPF in the 5G CUPS Wireless Network Architecture



The MX as SAEGW-U, SGW-U, PGW-U or UPF supports the following CUPS interfaces:

- **Sxab/Sxa/Sxb/N4**—Packet Forwarding Control Protocol (PFCP) enables communication between the Junos Multi-Access User Plane and the control plane. PFCP encodes TLV messages for transport over UDP/IP. This interface can also transport user data packets (GTP-U based) between the user plane and control plane. Junos Multi-Access User Plane runs PFCP as the control protocol with the third-party control plane to set up data paths for wireless subscribers.
- **S1-U/N3**—This interface is the data path between an eNodeB and the Junos Multi-Access User Plane. Application data packets from end-user equipment are encapsulated over GTP. For upstream packets, Junos Multi-Access User Plane is responsible for GTP tunnel termination and forwarding the user packets to the core. For downstream packets from core, Junos Multi-Access User Plane adds the GTP header and forwards to eNodeB(s). The data plane handles IP packets encapsulated in GTP-U from/to eNodeBs that arrive for the mobile subscribers and performs routing to/from the external Internet.
- **S5/8-U**—The S5/8-U interface is the data path between an SGW-U and a PGW-U.
- **N9**—Interface between two UPFs.
- **SGi/N6**—Interface to the core Internet, supporting IPv4.

Junos Multi-Access User Plane provides purely the user plane function in the form of an MX router that interacts with a third-party control plane function. The MX router receives instructions from the control plane through the Sxab/Sxa/Sxb/N4 interface using PFCP. Based on those instructions, the MX routing engine manages user plane sessions and programs data paths in the anchor PFEs. For the MX router to provide the user plane functionality, 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 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 Sxab/Sxa/Sxb/N4 interface in the CUPS architecture. The signalling/control interface is a physical interface that does the following:
 - Sends/receives PFCP packets to/from the control plane
- **At least one ingress interface**—This is the S1-U or N3 or the S5/8-U or N9 interface in the CUPS architecture, depending on where the device is in the data stream. The ingress interface is a physical interface that does the following:
 - As the S1-U or N3 interface, forwards GTP-U packets between eNodeBs and the anchor PFE.
 - As the S5/8-U or N9 interface, receives GTP-U packets from the downstream UPF.
- **At least one egress interface**—This is the SGi or N6 or the S5/8-U or N9 interface in the CUPS architecture, depending on where the device is in the data stream. The egress interface is a physical interface that does the following:
 - As the SGi or N6 interface, forwards IPv4 packets between the anchor PFE and the core network.
 - As the S5/8-U or N9 interface, sends GTP-U packets to the upstream UPF.

NOTE: You can configure all interface types on the same line card, as long as that line card supports all of the interface types. See [Table 1 on page 12](#) for a list of line card support by interface type.

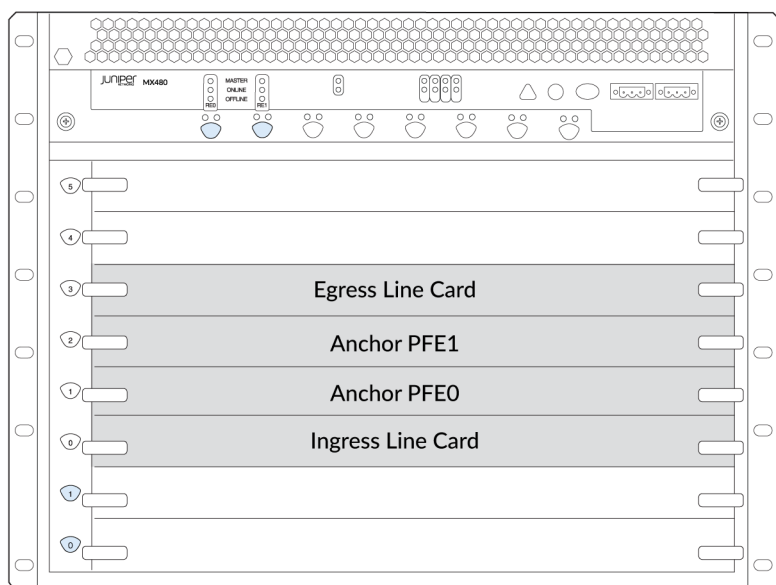
Configuring Junos Multi-Access User Plane on an MX Router

IN THIS SECTION

- [DDoS Attack Protection Configuration | 36](#)
- [GRES Configuration | 36](#)
- [Chassis Configuration for the Anchor PFE Line Cards | 37](#)
- [Interface Configuration | 37](#)
- [Mobile Edge Configuration | 39](#)

As [Figure 15 on page 35](#) shows, a standard setup of an MX router as either an SAEGW-U, an SGW-U, a PGW-U, or a UPF includes an ingress line card, and egress line card, and a recommended two anchor PFE line cards operating redundantly.

Figure 15: Standard setup for MX router as Junos Multi-Access User Plane



- The ingress line card provides the S1-U interface (SAEGW-U, SGW-U), the S5/8-U interface (PGW-U), or the N3 interface (UPF). , The ingress line card also provides the Sxab interface (SAEGW-U), the Sxa interface (SGW-U), the Sxb interface (PGW-U), or the N4 interface (UPF).

- 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 (SAEGW-U, PGW-U), the S5/8-U interface (SGW-U), or the N6 interface (UPF).
- You can configure all of this functionality on a single line card as long as that line card supports all of the Junos Multi-Access User Plane functionality. We show separate line cards here for simplicity and recommended setup.

To configure Junos Multi-Access User Plane on an MX router, perform the following configuration procedures in the listed order:

DDoS Attack Protection Configuration

Define DDoS attack protection for PFCP protocol traffic.

1. Configure protection for the PFCP protocol.

```
[edit system ddos-protection protocols]
user@host# set pfcf aggregate bandwidth packets-per-second
user@host# set pfcf aggregate burst size
user@host# set pfcf aggregate recover-time seconds
```

2. Configure GTP path management protection.

```
[edit system ddos-protection protocols]
user@host# set gtp-path-mgmt aggregate bandwidth packets-per-second
user@host# set gtp-path-mgmt aggregate burst size
user@host# set gtp-path-mgmt aggregate recover-time seconds
user@host# commit
```

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.

Configure Graceful Restart (GRES).

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

SEE ALSO

[GRES on Junos Multi-Access User Plane](#) | 23

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. Enable enhanced IP network services.

```
[edit chassis]
user@host# set network-services enhanced-ip
```

2. Configure slots for anchor PFE processing.

```
[edit chassis]
user@host# set fpc anchor-pfe0-slot pfe 0 forwarding-packages mobility user-plane
user@host# set fpc anchor-pfe0-slot pfe 1 forwarding-packages mobility user-plane
user@host# set fpc anchor-pfe1-slot pfe 0 forwarding-packages mobility user-plane
user@host# set fpc anchor-pfe1-slot pfe 1 forwarding-packages mobility user-plane
user@host# commit
```

Interface Configuration

Configure the interfaces needed.

1. Define the egress interface (SGi, S5/8-U, or N6). This interface is on the egress line card.

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

2. Define the interface that connects to the control plane function (Sxab, Sxa, Sxb, or N4). This interface is on the ingress line card.

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

3. Define the ingress interface (S1-U, S5/8-U, N3). This interface is on the ingress line card.

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

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 control planes, define the local address under the ["control-plane-peers" on page 76](#) stanza for each control plane function (CPF) 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 UPF.

1. Configure the connection to the control plane.

```
[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 control planes, define the local address under the control-plane-peers stanza for each CPF. The loopback address, however, is still required for Lawful Intercept to function.

2. Configure the connection to the access network through the S1-U or N3 interface, if applicable.

```
[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. Configure the connection to the core network peers through the S5/8-U or N9 interface, if applicable.

```
[edit services mobile-edge gateways saegw gateway-name core-network-peers]
user@host# set local-address local-address
user@host# set routing-instance routing-instance-name
user@host# set path-management enable
user@host# set t3-response seconds
```

- 4. 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
```

RELATED DOCUMENTATION

- [Anchor PFEs and Redundancy in Junos Multi-Access User Plane | 41](#)
- [Example: Configuring an MX Router as an SAEGW-U | 45](#)

Release History Table

Release	Description
21.3R1	Starting in Junos OS Release 21.3R1, Junos Multi-Access User Plane provides a long-route implementation as a replacement for a filter-based implementation to steer traffic to the anchor Packet Forwarding Engine removing the need for a firewall filter to route GTP packets.

Anchor PFEs and Redundancy in Junos Multi-Access User Plane

IN THIS SECTION

- [Understanding the Anchor PFE | 41](#)
- [Configuring No Redundancy for the Anchor PFEs | 41](#)
- [Configuring 1:1 Hot-standby Redundancy for the Anchor PFEs | 42](#)

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 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 and slot 2 for anchor processing.

```
[edit chassis]
user@host# set fpc 0 pfe 0 forwarding-packages mobility user-plane
user@host# set fpc 1 pfe 0 forwarding-packages mobility user-plane
```

2. Configure interfaces in slot 1 and 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 example:

- 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

Example: Configuring an MX Router as an SAEGW-U

IN THIS SECTION

- [Requirements | 45](#)
- [Overview | 47](#)
- [Configuration | 48](#)
- [Verification | 55](#)

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

NOTE: This example is also valid for configuring an MX Series Router as a UPF for 5G sessions. Junos Multi-Access User Plane can support 4G and 5G sessions simultaneously.

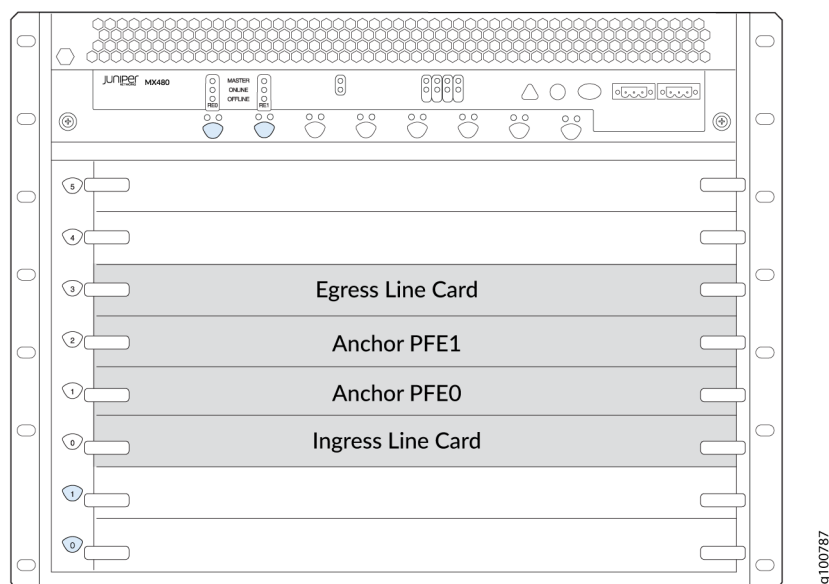
Requirements

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 21.3R1 or later

Figure 16 on page 46 below shows the hardware for this example.

Figure 16: 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 least one eNodeB
- Access to a packet data network (PDN)

Overview

IN THIS SECTION

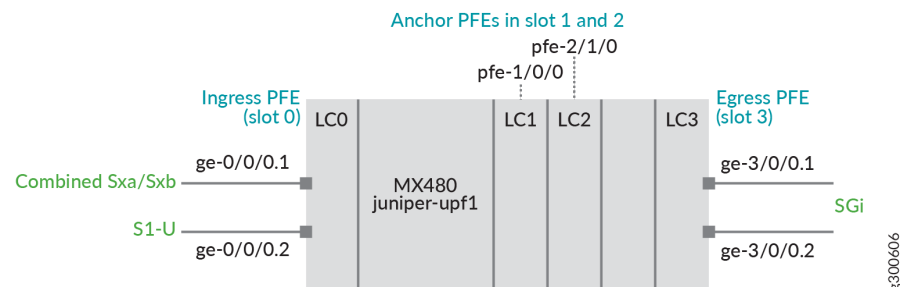
- [Topology | 47](#)

Topology

In this example (see [Figure 17 on page 47](#)):

- 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 17: Configuring an MX Router as an SAEGW-U



Configuration

IN THIS SECTION

- [CLI Quick Configuration | 48](#)
- [Procedure | 49](#)
- [Results | 52](#)

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 system ddos-protection protocols pfc aggregate bandwidth 20000
set system ddos-protection protocols pfc aggregate burst 9000
set system ddos-protection protocols pfc aggregate recover-time 30
set system ddos-protection protocols gtp-path-mgmt aggregate bandwidth 8400
set system ddos-protection protocols gtp-path-mgmt aggregate burst 8400
set system ddos-protection protocols gtp-path-mgmt aggregate recover-time 30
set chassis redundancy graceful-switchover
set chassis fpc 1 pfe 0 forwarding-packages mobility user-plane
set chassis fpc 2 pfe 1 forwarding-packages mobility user-plane
set chassis network-services enhanced-ip
set interfaces ge-0/0/0 vlan-tagging
set interfaces ge-0/0/0 unit 1 vlan-id 101
set interfaces ge-0/0/0 unit 2 vlan-id 102
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-3/0/0 vlan-tagging
set interfaces ge-3/0/0 unit 1 vlan-id 101
set interfaces ge-3/0/0 unit 2 vlan-id 102
set interfaces ge-3/0/0 unit 1 family inet address 30.0.1.1/24
set interfaces ge-3/0/0 unit 2 family inet address 30.0.2.1/24
set interfaces lo0 unit 0 family inet address 100.0.0.1/32
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

```

Procedure

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. Enable DDoS attack protection for PFCP protocol traffic.

```

[edit system ddos-protection protocols]
user@host# set pfc aggregate bandwidth 20000
user@host# set pfc aggregate burst 9000
user@host# set pfc aggregate recover-time 30
user@host# set gtp-path-mgmt aggregate bandwidth 8400
user@host# set gtp-path-mgmt aggregate burst 8400
user@host# set gtp-path-mgmt aggregate recover-time 30

```

2. Configure Graceful Restart (GRES).

```

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

```

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

```
[edit chassis]
user@host# set fpc 1 pfe 0 forwarding-packages mobility user-plane
user@host# set fpc 2 pfe 1 forwarding-packages mobility user-plane
```

4. Enable enhanced IP network services.

```
[edit chassis]
user@host# set network-services enhanced-ip
```

5. Configure the ingress logical interfaces using vlans.

```
[edit interfaces ge-0/0/0]
user@host# set vlan-tagging
user@host# set unit 1 vlan-id 101
user@host# set unit 2 vlan-id 102
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
```

6. 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
user@host# set unit 1 vlan-id 101
user@host# set unit 2 vlan-id 102
user@host# set unit 1 family inet address 30.0.1.1/24
user@host# set unit 2 family inet address 30.0.2.1/24
```

7. Configure the loopback address and the mobile interface for subscriber VRFs.

```
[edit interfaces lo0]
user@host# set unit 0 family inet address 100.0.0.1/32
[edit interfaces mif]
user@host# set unit 0 family inet
user@host# set unit 1 family inet
```

8. 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
```

9. Name the SAEGW-U gateway juniper-upf1 and 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]
user@host# set saegw juniper-upf1 control-plane-peers local-address 10.0.0.1
[edit services mobile-edge gateways saegw juniper-upf1 control-plane-peers]
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
```

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

NOTE: This is done at a different command hierarchy from the previous step.

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

11. Configure aggregate interface apfe0 for PFCP processing.

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

12. 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

```

Results

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

```

user@host# show system
ddos-protection {
  protocols {
    gtp-path-mgmt {
      aggregate {
        bandwidth 8400;
        burst 8400;
        recover-time 30;
      }
    }
    pfc {
      aggregate {
        bandwidth 20000;
        burst 9000;
        recover-time 30;
      }
    }
  }
}

```

```

user@host# show chassis
redundancy {
  graceful-switchover;
}
fpc 1 {
  pfe 0 {
    forwarding-packages {
      mobility {
        user-plane;
      }
    }
  }
}

```

```

    }
}
fpc 2 {
    pfe 1 {
        forwarding-packages {
            mobility {
                user-plane;
            }
        }
    }
}
network-services {
    enhanced-ip;
}

```

```

user@host# show interfaces
ge-0/0/0 {
    vlan-tagging {
        unit 1 {
            vlan-id 101;
        }
        unit 2 {
            vlan-id 102;
        }
    }
    unit 1 {
        family inet {
            address 10.0.0.1/24;
        }
    }
    unit 2 {
        family inet {          address 20.0.0.1/24;
        }
    }
}
ge-3/0/0 {
    vlan-tagging {
        unit 1 {
            vlan-id 101;
        }
        unit 2 {

```

```

        vlan-id 102;
    }
}
unit 1 {
    family inet {
        address 30.0.1.1/24;
    }
}
unit 2 {
    family inet {
        address 30.0.2.1/24;
    }
}
}
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;
  }
}
}
}

```

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

Verification

IN THIS SECTION

- [Verify SAEGW-U State | 56](#)
- [Verify SAEGW-U Peers | 56](#)
- [Verify SAEGW-U Sessions | 57](#)

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:      10.0.0.0
  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:      20.0.0.0
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: 10.0.0.2 Access-peer: 20.0.0.2
  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: 10.0.0.2 Access-peer: 20.0.0.2
  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: 10.0.0.2 Access-peer: 20.0.0.2
  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: 10.0.0.2 Access-peer: 20.0.0.2
  Anchor-PFE: apfe0:pfe-1/0/0 Secondary-anchor-PFE: apfe0:pfe-2/1/0
  Local-SEID: 0x2001d53 Remote-SEID: 0x4462
```

....

Release History Table

Release	Description
21.3R1	Starting in Junos OS Release 21.3R1, Junos Multi-Access User Plane provides a long-route implementation as a replacement for a filter-based implementation to steer traffic to the anchor Packet Forwarding Engine removing the need for a firewall filter to route GTP packets.

RELATED DOCUMENTATION

[Anchor PFEs and Redundancy in Junos Multi-Access User Plane | 41](#)

[MX Series Router As Junos Multi-Access User Plane | 31](#)

3

CHAPTER

Configuration Statements

apn-services (control plane services) | 61

forwarding-packages | 62

mobility | 64

peer-groups (access network peers) | 66

peer-groups (control plane peers) | 68

peer-groups (core network peers) | 70

saegw | 72

saegw access-network-peers | 74

saegw control-plane-peers | 76

saegw-core-network-peers | 79

saegw system | 82

apn-services (control plane services)

IN THIS SECTION

- [Syntax | 61](#)
- [Hierarchy Level | 61](#)
- [Description | 61](#)
- [Options | 62](#)
- [Required Privilege Level | 62](#)
- [Release Information | 62](#)

Syntax

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

Hierarchy Level

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

Description

The access point name (APN) is sent by the control plane over PFCP to place a subscriber in a specific network instance.

Options

apn name At least one access point name.

Required Privilege Level

system

Release Information

Statement introduced in Junos OS Release 19.4R1.

forwarding-packages

IN THIS SECTION

- [Syntax | 62](#)
- [Hierarchy Level | 63](#)
- [Description | 63](#)
- [Required Privilege Level | 63](#)
- [Release Information | 63](#)

Syntax

```
forwarding-packages {  
  mobility {  
    user-plane;  
    sgw;
```

```
}
}
```

Hierarchy Level

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

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.

Release Information

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

mobility

IN THIS SECTION

- [Syntax | 64](#)
- [Hierarchy Level | 64](#)
- [Description | 64](#)
- [Options | 65](#)
- [Required Privilege Level | 65](#)
- [Release Information | 65](#)

Syntax

```
mobility {  
    user-plane;  
    sgw;  
  
}
```

Hierarchy Level

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

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 user-plane forwarding package at the [edit unified-edge gateways user-plane *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

user-plane 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).

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

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

ggsn-pgw option deprecated and replaced with *user-plane* option in Junos OS Release 20.4R1.

RELATED DOCUMENTATION

[forwarding-packages](#) | [62](#)

peer-groups (access network peers)

IN THIS SECTION

- [Syntax](#) | [66](#)
- [Hierarchy Level](#) | [66](#)
- [Description](#) | [67](#)
- [Options](#) | [67](#)
- [Required Privilege Level](#) | [67](#)
- [Release Information](#) | [67](#)

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]
```

Description

Define a group of eNodeBs for an SAEGW-U or SGW-U.

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 user plane function during session establishment. The eNodeB is bound to the routing instance within the peer-groups stanza, if available. Otherwise, the user plane function uses the routing instance under "[access-network-peers](#)" on page 74.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

system

Release Information

Statement introduced in Junos OS Release 19.4R1.

peer-groups (control plane peers)

IN THIS SECTION

- [Syntax | 68](#)
- [Hierarchy Level | 68](#)
- [Description | 69](#)
- [Options | 69](#)
- [Required Privilege Level | 70](#)
- [Release Information | 70](#)

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]
```

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" on page 76](#).

Options

name	Peer group name
heartbeat-interval	Time between origination of two successive heartbeat requests (seconds). <ul style="list-style-type: none"> • Range: 60 through 255 • Default: 60
n3-requests	Maximim number of retries of PFCP request messages upon t3-response timeout. <ul style="list-style-type: none"> • Range: 1 through 5 • Default: 3
path-management	Enable/disable origination of heartbeat message requests to control peers. <ul style="list-style-type: none"> • 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). <ul style="list-style-type: none"> • Range: 1 through 5 • Default: 5

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

system

Release Information

Statement introduced in Junos OS Release 19.4R1.

peer-groups (core network peers)

IN THIS SECTION

- [Syntax | 70](#)
- [Hierarchy Level | 71](#)
- [Description | 71](#)
- [Options | 71](#)
- [Required Privilege Level | 71](#)
- [Release Information | 72](#)

Syntax

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

Hierarchy Level

```
[edit services mobile-edge gateways saegw name core-network-peers]
```

Description

Define a peer group of PGW-Us for an SGW-U or a group of SGW-Us for a PGW-U.

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, peers matching only this address/prefix are accepted by the user plane function during session establishment. The peer is bound to the routing instance within the peer-groups stanza, if available. Otherwise, the user plane function uses the routing instance under "[saegw-core-network-peers](#)" on page 79.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

system

Release Information

Statement introduced in Junos OS Release 20.4R1.

saegw

IN THIS SECTION

- [Syntax | 72](#)
- [Hierarchy Level | 73](#)
- [Description | 73](#)
- [Options | 73](#)
- [Required Privilege Level | 73](#)
- [Release Information | 73](#)

Syntax

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

Hierarchy Level

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

Description

Define the gateway name.

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

Options

name	Gateway name
-------------	--------------

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

system

Release Information

Statement introduced in Junos OS Release 19.4R1.

core-network-peers option introduced in Junos OS Release 20.4R1.

saegw access-network-peers

IN THIS SECTION

- [Syntax | 74](#)
- [Hierarchy Level | 74](#)
- [Description | 75](#)
- [Options | 75](#)
- [Required Privilege Level | 75](#)
- [Release Information | 76](#)

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]
```

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/SGW-U during session establishment. The eNodeB is bound to the routing instance within the "[peer-groups](#)" on page 66 stanza, if available. Otherwise, the SAEGW-U/SGW-U uses the routing instance provided here.

t3-response

Waiting time 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

Release Information

Statement introduced in Junos OS Release 19.4R1.

RELATED DOCUMENTATION

[saegw control-plane-peers](#) | 76

[saegw-core-network-peers](#) | 79

saegw control-plane-peers

IN THIS SECTION

- [Syntax](#) | 76
- [Hierarchy Level](#) | 77
- [Description](#) | 77
- [Options](#) | 77
- [Required Privilege Level](#) | 79
- [Release Information](#) | 79

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]
```

Description

Use this section to define the connection to and characteristics of control plane peers (SAEGW-C, SGW-C, or PGW-C).

Options

heartbeat-interval	Time between two successive heartbeat requests (seconds).
	<ul style="list-style-type: none"> • 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 control plane peers, define the local address under the `control-plane-peers` stanza for each control plane peer 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

Release Information

Statement introduced in Junos OS Release 19.4R1.

RELATED DOCUMENTATION

[saegw access-network-peers](#) | 74

[saegw-core-network-peers](#) | 79

saegw-core-network-peers

IN THIS SECTION

- [Syntax](#) | 80
- [Hierarchy Level](#) | 80
- [Description](#) | 80
- [Options](#) | 80
- [Required Privilege Level](#) | 81
- [Release Information](#) | 81

Syntax

```
core-network-peers {
    echo-interval seconds;
    local-address [ local-address ... ];
    n3-requests n3-requests;
    path-management (disable | enable);
    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]
```

Description

Define core-facing GTP-U peers (SGW-U to PGW-U and vice versa).

Options

echo-interval Time between origination of two successive echo requests (seconds). You must enable path-management for echo requests to occur.

- **Range:** 60 through 255

	<ul style="list-style-type: none"> • Default: 60
local-address	Required. IPv4 address(es) of the local end of the GTP-U connection.
n3-requests	<p>Number of retries of peer management request messages upon t3-response timeout.</p> <ul style="list-style-type: none"> • Range: 1 through 5 • Default: 3
path-management	<p>Enable/disable origination of echo requests to core peers.</p> <ul style="list-style-type: none"> • Default: Disabled
routing-instance	Local routing instance of the GTP-U connection.
t3-response	<p>Waiting time before retrying peer management request upon response timeout (seconds).</p> <ul style="list-style-type: none"> • Range: 1 through 5 • Default: 5

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

system

Release Information

Statement introduced in Junos OS Release 20.4R1.

RELATED DOCUMENTATION

[saegw access-network-peers](#) | 74

[saegw control-plane-peers](#) | 76

saegw system

IN THIS SECTION

- [Syntax | 82](#)
- [Hierarchy Level | 82](#)
- [Description | 83](#)
- [Options | 83](#)
- [Required Privilege Level | 83](#)
- [Release Information | 83](#)

Syntax

```
system {  
  anchor-pfes {  
    interface interface-name {  
      colocated-4g-pgw;  
      colocated-4g-sgw;  
    }  
  }  
}
```

Hierarchy Level

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

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*
- colocated-4g-pgw** (Optional) Attach the PGW-U gateway type to the anchor PFE to optimize throughput of 4G traffic.
- colocated-4g-sgw** (Optional) Attach the SGW-U gateway type to the anchor PFE to optimize throughput of 4G traffic.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

system

Release Information

Statement introduced in Junos OS Release 19.4R1.

colocated-4g-pgw and **colocated-4g-sgw** options introduced in Junos OS Release 21.3R1.

4

CHAPTER

Operational Commands

`show services mobile-edge peers` | 85

`show services mobile-edge sessions` | 89

`show services mobile-edge summary` | 104

show services mobile-edge peers

IN THIS SECTION

- [Syntax | 85](#)
- [Description | 85](#)
- [Options | 85](#)
- [Required Privilege Level | 86](#)
- [Output Fields | 86](#)
- [Sample Output | 87](#)
- [Release Information | 89](#)

Syntax

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

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

Output Fields

Table 3 on page 86 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 3: show services mobile-edge peers Output Fields

Field Name	Field Description
Peers Summary	<p>The Peers Summary field provides the following information:</p> <ul style="list-style-type: none">• Total number of control (SAEGW-C) peers.• Total number of access network peers.• Total rejected association setup requests.
Control Peer Information	<p>The Control Peer Information field provides the following information about each SAEGW-C:</p> <ul style="list-style-type: none">• IP address• Hostname• Routing-Instance• Peer Group name

Table 3: show services mobile-edge peers Output Fields (Continued)

Field Name	Field Description
Access Peer Information	<p>The Access Peer Information field provides the following information about each access network peer:</p> <ul style="list-style-type: none"> • IP address • Hostname • Routing-Instance • Peer Group name
Control Peer Statistics	<p>The Control Peer Statistics field provides the following statistics about each SAEGW-C:</p> <ul style="list-style-type: none"> • 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	<p>The Access Peer Statistics field provides the following statistics about each access network peer:</p> <ul style="list-style-type: none"> • 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

```

Release Information

Command introduced in Junos OS 19.4R1.

RELATED DOCUMENTATION

[Example: Configuring an MX Router as an SAEGW-U | 45](#)

show services mobile-edge sessions

IN THIS SECTION

- [Syntax | 90](#)
- [Description | 90](#)
- [Options | 90](#)
- [Required Privilege Level | 91](#)
- [Output Fields | 91](#)

- Sample Output | 94
- Release Information | 103

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 | core-network-peers | pic |
slot | slot>
```

Description

This command gives information on mobile sessions active on the SAEGW-U/SGW-U/PGW-U/UPF.

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/SGW-U/PGW-U/UPF.
-------------	---

control-plane-peers	Display information on mobile sessions for a specific or all SAEGW-Cs/SGW-C/PGW-C/SMF.
detail	Display detailed information on mobile sessions or on a specific SAEGW-C/SGW-C/PGW-C/SMF.
extensive	Display extensive information on mobile sessions or by local SEID.
summary	Display summary information on mobile sessions active on the SAEGW-U/SGW-U/PGW-U/UPF.
access-network-peers	Display session summary output by access network peer.
core-network-peers	Display session summary output by core 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.
statistics	Display detailed session statistics.

Required Privilege Level

view

Output Fields

[Table 4 on page 92](#) 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 4: 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.
Num-QoS-Flows	Number of 5G QoS flows 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 control plane peer for the session.
Access-peer	IP address of the access peer (eNodeB) for the session.
Core-peer	IP address of the core network peer 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.
User ID	IE that can be present in a PFCP Session Establishment Request. This IE is useful for troubleshooting problems in the UPF affecting a subscriber.
Bearer EBI/NSAPI	EPS Bearer ID / Network Service Access Point Identifier.

Table 4: show services mobile-edge sessions Output Fields (Continued)

Field Name	Field Description
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.
Beareres by State	The current number of bearers in state: BEARER_WAIT, ESTABLISHED, DELETING, and Total.

Table 4: show services mobile-edge sessions Output Fields (Continued)

Field Name	Field Description
Bearers by Downlink FAR state	<p>The current number of bearers by downlink FAR state. The allowable states are:</p> <ul style="list-style-type: none"> • FORWARD– Downlink FAR apply action is set to Forward. • DROP – Downlink FAR apply action is set to Drop. • IDLE – Downlink FAR apply action is set to Notify Control Plane and/or Buffer, but the first packet has not been detected by the PFE. • BUFFER - Downlink FAR apply action is set to Notify Control Plane and/or Buffer, and the first packet has been detected by the PFE.
APFE PIC	The anchor PFE PIC.
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 Core-peer: 30.4.1.2
    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 Core-peer: 30.4.1.2
    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 Core-peer: 30.4.1.2
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 Core-peer: 30.4.1.2
```

```
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
```

```
Num-QoS-Flows: 2
```

```
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
```

```
Num-QoS-Flows: 2
```

```
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
```

```
Num-QoS-Flows: 2
```

```
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
 Num-QoS-Flows: 2
 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**

State: ESTABLISHED Num-bearers: 2
 Num-QoS-Flows: 2
 VRF-ID: 0x0 APN: default
 CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6 Core-peer: 30.4.1.2
 Anchor-PFE: apfe0:pfe-3/0/0 Secondary-anchor-PFE: apfe0:pfe-2/0/0
 Local-SEID: 0x100012e Remote-SEID: 0x2711

Bearer EBI/NSAPI: 5 State: ESTABLISHED
 Access Loc TEID: 0x100000 Rem TEID: 0x1f4242
 Core Loc TEID: 0x100010 Rem TEID: 0xfda42

Bearer EBI/NSAPI: 6 State: ESTABLISHED
 Access Loc TEID: 0x100001 Rem TEID: 0x1f4243
 Core Loc TEID: 0x100011 Rem TEID: 0xfda43

State: ESTABLISHED Num-bearers: 1
 Num-QoS-Flows: 2
 VRF-ID: 0x0 APN: default
 CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6 Core-peer: 30.4.1.2
 Anchor-PFE: apfe0:pfe-3/0/0 Secondary-anchor-PFE: apfe0:pfe-2/0/0
 Local-SEID: 0x12d Remote-SEID: 0x2710

Bearer EBI/NSAPI: 5 State: ESTABLISHED
 Access Loc TEID: 0x400000 Rem TEID: 0x1f4240
 Core Loc TEID: 0x400010 Rem TEID: 0xfda40

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
```

```
Num-QoS-Flows: 2
```

```
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
```

```
Num-QoS-Flows: 2
```

```
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
```

```
Num-QoS-Flows: 2
```

```
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
```

```
State: ESTABLISHED Num-bearers: 1
```

```
Num-QoS-Flows: 2
```

```
VRF-ID: 0x0 APN: default
```

CPF-peer: 20.3.1.3 Access-peer: 10.4.1.6 Core-peer: 30.4.1.2
 Anchor-PFE: apfe0:pfe-3/0/0 Secondary-anchor-PFE: apfe0:pfe-2/0/0
 Local-SEID: 0x12d Remote-SEID: 0x2710
 User ID:
 IMSI : 313460000000001
 IMEI : 359411081675635
 MSISDN: 16173434500
 NAI : johndoe@foonet.com

Bearer EBI/NSAPI: 5 State: ESTABLISHED
 Access Loc TEID: 0x400000 Rem TEID: 0x1f4240
 Core Loc TEID: 0x400010 Rem TEID: 0xfda40

FAR-ID: 1
 Destination Interface: Core
 Apply Action: Forward

FAR-ID: 2
 Destination Interface: Access
 Apply Action: Notify CP, Buffer

PDR ID: 2

FAR ID: 2

QER ID: 1
 Uplink gate : Open Downlink gate : Open
 Uplink mbr : 5000 kbps Downlink mbr : 5000 kbps
 SDF Filter:
 permit out ip from any to assigned

PDR ID: 1

FAR ID: 1

QER ID: 1
 Uplink gate : Open Downlink gate : Open
 Uplink mbr : 5000 kbps Downlink mbr : 5000 kbps
 SDF Filter:
 permit out ip from any to assigned

URR ID: 0x1
 Measurement Method: Volume

Reporting Trigger: Dropped Downlink Traffic Threshold
 Dropped DL traffic threshold: 800000 octets

Usage report trigger: Volume Threshold
 Usage report start timestamp: Tue Feb 25 18:12:18 2020 UTC
 Usage report stop timestamp: Tue Feb 25 18:24:38 2020 UTC

URR ID: 0x2

Measurement Method: Volume
 Reporting Trigger: Volume Threshold
 Uplink volume threshold: 800000 octets
 Downlink volume threshold: 800000 octets
 Total volume threshold: 800000 octets
 Measurement Information: Inactive

URR statistics:

URR messages:

URR ID	Usage Report Count	Last Report Timestamp
0x1	1	Tue Feb 25 18:12:18 2020

Session Reports:

Type	Report Count	Last Report Timestamp
Usage	1	Tue Feb 25 18:12:18 2020
Downlink Data	1	Tue Feb 25 16:52:11 2020
Error Indication	1	Tue Feb 25 22:12:17 2020
Total	3	

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

Bearers by Downlink FAR state:


```
FORWARD: 1467
IDLE: 452
BUFFERING: 81
Total: 2000
```

5G QoS Flows by State:

```
WAIT: 2
Total: 2
```

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

Beareres 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

Beareres by State:

ESTABLISHED: 6421

DELETING: 4832

Total: 11253

Summary by Access Point Names:

APN: test.internet.488

Sessions by State:

Total: 0

Beareres 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

Beareres 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

Beareres 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

Beareres 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

```

Release Information

Command introduced in Junos OS 19.4R1.

core-network-peers option introduced in Junos OS 20.4R1.

RELATED DOCUMENTATION

[Example: Configuring an MX Router as an SAEGW-U](#) | 45

show services mobile-edge summary

IN THIS SECTION

- [Syntax | 104](#)
- [Description | 104](#)
- [Required Privilege Level | 104](#)
- [Output Fields | 104](#)
- [Sample Output | 105](#)
- [Release Information | 105](#)

Syntax

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

Description

This command gives summary information on the SAEGW-U.

Required Privilege Level

view

Output Fields

[Table 5 on page 105](#) 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 5: show services mobile-edge summary Output Fields

Field Name	Field Description
Graceful-Restart	Whether graceful-restart is enabled or disabled.
Primary Role	Primary Role state for the given routing engine (RE) this command is executed on. For the primary 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

```

Release Information

Command introduced in Junos OS 19.4R1.

RELATED DOCUMENTATION

[Example: Configuring an MX Router as an SAEGW-U](#) | 45