

# Junos<sup>®</sup> OS 12.1W Mobility Release Notes

Release 12.1W  
22 August 2012  
Revision 1

These release notes accompany Release 12.1W of the Junos OS for the MobileNext Broadband Gateway. They describe device documentation and known problems with the software. Junos OS for the MobileNext Broadband Gateway runs on all Juniper Networks MX Series Ethernet Services routers except the MX80 router and lower.

For the latest, most complete information about outstanding and resolved issues with the Junos OS for the MobileNext Broadband Gateway software, see the Juniper Networks online software defect search application at <http://www.juniper.net/prsearch>.

## Contents

New Features in Junos OS Release 12.1W for MobileNext Broadband Gateway . . . . .	3
Diameter . . . . .	3
Policy and Charging Enforcement Function . . . . .	4
Charging . . . . .	5
Changes in Default Behavior in Junos OS Release 12.1W for the MobileNext Broadband Gateway . . . . .	9
Resolved Issues in Junos OS Release 12.1W for the MobileNext Broadband Gateway . . . . .	10
Gateway . . . . .	10
Chassis . . . . .	10
GTP . . . . .	10
QoS/CAC . . . . .	11
Issues in Junos OS Release 12.1W for the MobileNext Broadband Gateway . . . . .	11
Current Software Release . . . . .	11
Outstanding Issues in Junos OS Release 12.1W for the MobileNext Broadband Gateway . . . . .	11
Previous Software Release . . . . .	12
Outstanding Issues in Junos OS Release 12.1WB2 for the MobileNext Broadband Gateway . . . . .	12
Errata in Junos OS Release 12.1W for MobileNext Broadband Gateway . . . . .	14
Documentation . . . . .	14
General Information . . . . .	14
Requesting Technical Support . . . . .	14
Self-Help Online Tools and Resources . . . . .	14
Opening a Case with JTAC . . . . .	15

Copyrights .....	15
------------------	----

## New Features in Junos OS Release 12.1W for MobileNext Broadband Gateway

The following features have been added to Junos OS Release 12.1W for the MobileNext Broadband Gateway. Following the description is the title of the manual or manuals to consult for further information.

### Diameter

- **Diameter base protocol support (Broadband Gateway MX Series platforms)**—The Diameter protocol is defined in RFC 3588, *Diameter Base Protocol*, and provides basic services to one or more applications (also called functions). The individual application provides the extended functionality. The Gy application and the Gx application are currently supported.

Diameter peers communicate over a TCP transport layer connection by exchanging Diameter messages. The Diameter network element is similar to a peer group that provides function-specific features such as load balancing and failover procedures. Each Diameter network element can be associated with one or more functions and consists of a prioritized list of peers. Applications typically send requests to a network element rather than to a single peer.

Every Diameter node requires Origin-Host and Origin-Realm information to be included in all messages that originate from this Diameter instance.

To configure the origin node, include the **origin** statement at the **[edit access diameter]** hierarchy level. Specify the Origin-Realm AVP and Origin-Host prefix by including the **realm** and **host** statements at the **[edit access diameter origin]** hierarchy level.

To configure the Diameter transport used by the peer, include the **transport** statement at the **[edit access diameter]** hierarchy level. Specify the source address for the peer by including the **address** statement at the **[edit access diameter transport]** hierarchy level.

To configure the remote Diameter peers, include the **peer** statement at the **[edit access diameter]** hierarchy level, and then include the **address** and **connect-actively** statements at the **[edit access diameter peer peer-name]** hierarchy level.

To configure the Diameter network elements, include the **network-element** statement at the **[edit access diameter]** hierarchy level. Include the **function** statement at the **[edit diameter network-element element-name]** hierarchy level. Specify the peers associated with the Diameter network element by including one or more **peer** statements at the **[edit access diameter network-element element-name]** hierarchy level. Prioritize the peer by including the **priority** statement at the **[edit access diameter network-element element-name peer peer-name]** hierarchy level.

To display information about Diameter, you can issue the following commands:

- **show unified-edge ggsn-pgw diameter dcca-gy statistics**
- **show unified-edge ggsn-pgw diameter network-element statistics**
- **show unified-edge ggsn-pgw diameter network-element status**

- **show unified-edge ggsn-pgw diameter pcc-gx statistics**
- **show unified-edge ggsn-pgw diameter peer statistics**
- **show unified-edge ggsn-pgw diameter peer status**

*[MobileNext Broadband Gateway Configuration Guide]*

- **Diameter profiles (Broadband Gateway MX Series platforms)**—You can use Diameter profiles to send requests for a Gy application or a Gx application. The Diameter profiles reference a prioritized list of targets that reference Diameter network elements.

To configure Diameter profiles, include the **diameter-profiles** statement at the **[edit unified-edge]** hierarchy level. Specify the profile for the Gy application by including the **gy-profile** statement at the **[edit unified-edge diameter-profiles]** hierarchy level. Specify the profile for the Gx application by including the **gx-profile** statement at the **[edit unified-edge diameter-profiles]** hierarchy level.

To configure the target for the profile, include the **destination-realm**, **network-element**, and **priority** statements at the **[edit unified-edge diameter-profiles gy-profile profile-name targets target-name]** or **[edit unified-edge diameter-profiles gx-profile profile-name targets target-name]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

## Policy and Charging Enforcement Function

- **PCEF profiles**—A policy and charging enforcement function (PCEF) profile is used to enforce quality-of-service (QoS), charging, and gating control decisions. The policy decisions that the PCEF enforces are either predefined (using static policies) or are received from the PCRF (using dynamic [static Gx] policies). A PCEF profile is also used to provide the PCRF with user- and access-specific information over the Gx interface.

To configure the PCEF profiles, include the **profiles** statement at the **[edit unified-edge pcef]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Event triggers**—Event triggers can be configured to notify the policy and charging rules function (PCRF) about changes in the access network, so that when an event occurs that matches an event trigger configured on the PCEF, the PCEF reports the event to the PCRF. To configure event triggers, include the **event-trigger-profiles** statement at the **[edit unified-edge pcef]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Service Data Flow filters**—Service Data Flow filters are configured in a Policy and Charging Control (PCC) rule to classify subscriber IP packets to a service data flow.

To configure the Service Data Flow filters, include the **flow-descriptions** statement at the **[edit unified-edge pcef]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Policy and Charging Control (PCC) action profiles**—The PCC action profile is configured in a PCC rule to provide quality-of-service (QoS) control, charging control, and gating control for the subscriber IP packets associated with a service data flow.

To configure PCC action profiles, include the **pcc-action-profiles** statement at the **[edit unified-edge pcef]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Predefined policies**—PCC rules (and PCC rulebases) are configured as either static or dynamic predefined policies. Static policies are predefined PCC rules that are controlled by the PCEF, and activated and deactivated locally on the P-GW without any interaction with the PCRF server. Dynamic policies (*static Gx* policies) are predefined PCC rules that are configured on the PCEF, but are dynamically controlled (activated and deactivated) by the PCRF over the Gx interface. The PCRF provides the name of predefined dynamic policies to be activated or deactivated.

To configure PCC rules or PCC rulebases, include the **predefined-policies** statement at the **[edit unified-edge pcef]** hierarchy level.

To configure a PCC rule or rulebase as static policy, specify the name of the predefined rule or rulebase at the **[edit unified-edge pcef profiles profile-name static-policy-control]** hierarchy level.

To configure a PCC rule or rulebase as a dynamic (static Gx) policy, specify the name of the predefined rule or rulebase at the **[edit unified-edge pcef profiles profile-name dynamic-policy-control]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

- **PCEF profiles**—The PCEF profile is used to enforce QoS, charging, and gating control decisions. The policy decisions that the PCEF enforces are either predefined (using static policies) or are received from the PCRF (using dynamic policies). A PCEF profile is also used to provide the PCRF with user- and access-specific information over the Gx interface.

To configure the PCEF profiles, include the **profiles** statement at the **[edit unified-edge pcef]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

## Charging

- **Support for online charging (broadband gateway MX Series platforms)**—The broadband gateway now supports online charging and associated features for mobility, which enables real-time charging of subscribers. Support for online charging includes policy and charging rules, quality-of-service (QoS) determination, credit control failure handling, and overall charging considerations. The Gy interface connects the P-GW and the online charging system (OCS).

*[MobileNext Broadband Gateway Configuration Guide]*

- **Requesting time or volume quotas from the OCS (broadband gateway MX Series platforms)**—You can configure the time or volume quota, per rating group or per service identifier within a rating group, in the requested service unit to be sent to the OCS. If

the PCRF does not specify a rating group, then the default rating group or default service identifier configured locally (for the charging profile) is used to request quota from the OCS. In addition, depending on the measurement method provided by the PCRF or locally configured for the trigger profile, either the time quota or volume quota is included in the requested service units sent to the OCS.

To configure the time and volume quotas to be requested from the OCS, include the **requested-service-unit** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name online]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Support for volume and wall clock time quota management (broadband gateway MX Series platforms)**—The broadband gateway supports time or volume quota per rating group or per service identifier within a rating group. The quota granted by the OCS is programmed for each rating group or service identifier and when it is exhausted, the gateway reauthorizes with the OCS. If the PCRF does not specify a rating group, then the default rating group or default service identifier configured locally (for the charging profile) is used to request quota from the OCS.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Service identifier-level quota support (broadband gateway MX Series platforms)**—The broadband gateway supports the granting of a separate quota for each service identifier under a rating group. The broadband gateway enforces the granted quota for each service of the rating group and reports the quota to the OCS when quota is exhausted or the session is terminated.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Support for signaling events per rating group (broadband gateway MX Series platforms)**—The broadband gateway supports the reauthorization of quota based on the signaling events (such as RAT change, ULI change, time zone change, and so on) specified by the OCS in the Trigger AVP in the Credit Control Answer (CCA) message.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Threshold-based reauthorization triggers (broadband gateway MX Series platforms)**—You can configure threshold-based reauthorization for reporting and requesting usage quota from the OCS. Unlike the quota threshold received from the OCS, the quota threshold configured in the trigger profile, which is used only if OCS does not provide a quota threshold or if an override is configured locally, ensures the same treatment for all subscriber types.

To configure threshold-based reauthorization triggers, include the **quota-threshold** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name online]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Reporting at rating group or service identifier level (broadband gateway MX Series platforms)**—You can configure the reporting of usage to the OCS at the rating group level, which is the cumulative usage across all the service identifiers in the rating group, or at the service identifier level, which is usage of each service identifier within the rating group. In the latter case, a separate Multiple-Services-Credit-Control (MSCC) AVP is

included for each service identifier (of the rating group) reporting its usage. Depending on the measurement method provided by the PCRF or locally configured for the trigger profile, either the time quota or volume quota is included in the requested service units sent to the OCS.

To configure the reporting level for reports to the offline charging gateway and the OCS, include the **reporting-level** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name online]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Redundancy support at the rating group level (broadband gateway MX Series platforms)**—The broadband gateway supports the synchronization of subscriber statistics to the backup session PIC to ensure that there is no loss of charging data.

The Packet Forwarding Engine sends the subscriber usage statistics to the session PIC that is currently active. The session PIC sends an acknowledgment to the Packet Forwarding Engine only after it sends the statistics to the OCS and the backup session PIC. In case of switchover to the backup session PIC, that is, the current active session PIC fails before sending the acknowledgment, then the Packet Forwarding Engine will resend the statistics to the new active session PIC. The new active session PIC then resends the CCR, with exact usage for all rating groups, to the OCS, ensuring that subscriber usage data is not lost.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Credit control failure handling actions (broadband gateway MX Series platforms)**—You can configure credit control failure handling parameters, which determine the actions that the broadband gateway performs when credit control failure occurs.

An online rating group can be converted to offline based on certain failure conditions. The failure conditions include the online charging system (OCS) not being reachable, a congested network, or receipt of specific result codes from the OCS. This ensures that offline CDR records are generated in cases of network congestion or down events.

Subscribers can also be granted grace quota for a limited usage (volume quota) or time limit (time quota). When the broadband gateway is unable to interact with the OCS, if the OCS is down or if the network is congested, then to avoid denial of service, the broadband gateway can grant grace quota so that the service is granted but limited to a specific volume quota, time quota, or both.

To configure the conversion of a subscriber to offline charging, include the **convert-to-offline** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name online cc-failure-handling]** hierarchy level.

To configure the grace quota (volume quota, time quota, or both) to be allocated in case quota is exhausted, include the **grace-quota** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name online]** hierarchy level.

To enable the granting of grace quota, include the **grant-grace-quota** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name online]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Blacklisting rating groups (broadband gateway MX Series platforms)**—You can configure the blacklisting of specific rating groups based on the Diameter Result-Code AVP from the OCS. When a rating group is blacklisted, all the packets for that rating group are dropped. The OCS must initiate a Re-Auth Request to remove the blacklist and re-enable traffic on the rating group.

To configure rating group blacklist support, include the **blacklist** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name online cc-failure-handling result-code-based-action authorization-rejected]** hierarchy level, the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name online cc-failure-handling result-code-based-action credit-limit-reached]** hierarchy level, or both hierarchy levels.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Preemptive quota support (broadband gateway MX Series platforms)**—The broadband gateway supports the receipt of quota for new rating groups or combination of rating group and service identifier, which was not requested in the Credit Control Request (CCR) message. The quotas are held until the rating groups are activated by PCEF policies and are returned to the OCS when the bearer is terminated. This reduces the extra signaling that would have been needed when the rating groups are activated without preemptive quota support.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Final unit action support (broadband gateway MX Series platforms)**—The broadband gateway supports the receipt of the final unit indication from the OCS. When the final units are exhausted, the final unit indication action is applied. This reduces the signaling between the P-GW and the OCS, since the P-GW need not request additional units after the final units are exhausted.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Integrated call admission control with Gy (broadband gateway MX Series platforms)**—The broadband gateway ensures that call admission control (CAC) mechanisms are applied when overload conditions are detected.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Display of online charging statistics (broadband gateway MX Series platforms)**—The outputs of the **show unified-edge ggsn-pgw apn statistics** and **show unified-edge ggsn-pgw subscribers** (detail and extensive options) commands now include online charging statistics.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Offline charging enhancements (broadband gateway MX Series platforms)**—The following are applicable to the broadband gateway configured as a GGSN or P-GW:

- **Enhanced CDR support (broadband gateway MX Series platforms)**—The broadband gateway now supports Release 7 eG-CDRs and Release 9 P-GW CDRs in addition to Release 7 G-CDRs and Release 8 P-GW CDRs

*[MobileNext Broadband Gateway Configuration Guide]*



- **Offline container and CDR generation support (broadband gateway MX Series platforms)**—The broadband gateway supports tight interworking between online and offline charging.

When both offline and online charging methods are used, the generation of containers and CDRs is driven by online triggers. When the online volume quota or time quota is exhausted, the Diameter Credit Control Application (DCCA) event trigger configuration determines when the container is generated and whether the CDR is closed or not. A rating group can be both online and offline at the same time, as indicated by the PCRF or based on the configuration on the gateway.

When only offline charging is used, the expiry of the volume limit or the time limit triggers closure of the CDR. In addition, when signaling events occur a container is generated if there is data traffic and the CDR is closed if the duration and data is non-zero; that is, only active containers are included in the CDR. (A container is open or active when there is data traffic for the rating group.)

When a bearer is terminated, all the rating groups of that bearer are included in the CDR.

To configure the exclusion of the generation of offline containers when DCCA events occur, include the **dcca-events** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name offline]** hierarchy level.

To configure volume limit or time limit triggers, which is already supported on the broadband gateway, include the **time-limit** or **volume-limit** statements at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name offline]** hierarchy level.

*[MobileNext Broadband Gateway Configuration Guide]*

- **Volume and time limit support at rating group level (broadband gateway MX Series platforms)**—The broadband gateway supports volume and time limits at the rating group level.

In the case of time limit or volume limit, the P-GW generates a CDR with a container, for that rating group. If the rating group has no traffic, then the container is skipped.

In case of signaling events (such as RAT change, MS time zone change, and so on), a CDR is generated with all rating groups included, only if the following conditions are met: no traffic containers are skipped, and there is at least one container with traffic, or the CDR duration is not zero. Otherwise, CDR generation is skipped.

*[MobileNext Broadband Gateway Configuration Guide]*

---

## Changes in Default Behavior in Junos OS Release 12.1W for the MobileNext Broadband Gateway

---

The changes to default behavior and syntax for the MobileNext Broadband Gateway are as follows:

- The **show unified-edge ggsn-pgw apn call-rate statistics** command includes the following statistics:

- Number of active prepaid bearers
- Number of active postpaid bearers
- Number of authorization attempts
- Number of online authorizations successful
- Number of online authorization timeouts
- Number of reauthorizations requests sent
- Number of server initiated reauthorizations received
- Number of successful reauthorizations

[PR/741288]

- If you configure a primary and secondary Packet Forwarding Engine under **[edit interfaces apfen anchoring-options]**, the secondary Packet Forwarding Engine cannot share the FPC with any of its primary Packet Forwarding Engines. In other words, if you configure **pfe-2/0/0** as a primary, you should not configure **pfe-2/1/0** as a secondary or you will get a commit warning. [PR/790847]

## Resolved Issues in Junos OS Release 12.1W for the MobileNext Broadband Gateway

---

The following are the issues that have been resolved for the MobileNext Broadband Gateway in this release. The identifier following the descriptions is the tracking number in the bug-tracking database.

### Chassis

- Wildcard configuration for mobile interfaces at the **[edit class-of-service]** hierarchy level does not work. As a workaround, configure specific mobile interfaces (for example, **mif.0**, **mif.1**, and so on). [PR/577828]
- Taking a Packet Forwarding Engine or anchor Packet Forwarding Engine group interface offline, putting a Packet Forwarding Engine or anchor Packet Forwarding Engine group interface online, or changing configuration parameters should be done using maintenance mode. [PR/660293]
- Moving **mams-** members across **ams** interfaces within a single configuration **commit** is not supported. As a workaround to move (for example) **mams-4/0/0** from **ams-1** to **ams-2**, you must remove a **mams-** interface member, commit, and then add it to another **ams-** interface. [PR/723582]

### GTP

When the GTP peer count hits 40,000 (40k), using the **show unified-edge ggsn-pgw gtp peer | count** command to count GTP peers causes a **mobiled** restart. As a workaround, use the **show unified-edge ggsn-pgw gtp peer count** command instead. In other words, do not include the pipe (|) symbol in the command. [PR/770626]

## QoS/CAC

If the value for the **anchor-pfe-default-bearers-percentage** statement at the **[edit unified-edge gateways sgw sgw-name]** hierarchy level of an S-GW is changed while the broadband gateway is running and the change committed, subsequent GTP create session requests from MMEs to the specific S-GW do not process successfully and result in reject responses sent to the MME. As a workaround, reboot the broadband gateway when you change the value of the **anchor-pfe-default-bearers-percentage** statement at the **[edit unified-edge gateways sgw sgw-name]** hierarchy level of an S-GW. [PR/702190]

---

## Issues in Junos OS Release 12.1W for the MobileNext Broadband Gateway

The current software release is Release 12.1W for Mobility.

- [Current Software Release on page 11](#)
- [Previous Software Release on page 12](#)

## Current Software Release

---

### Outstanding Issues in Junos OS Release 12.1W for the MobileNext Broadband Gateway

#### **APNs**

- The command **show unified-edge ggsn-pgw apn call-rate statistics** is not documented. [PR/741288]
- The **user-options** statement at the **[edit unified-edge ggsn-pgw gateway-name apn-services apns apn-name]** hierarchy level replaces the **anonymous-user** statement. [PR/756873]
- If you configure the **verify-source-address** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name apn-services apns apn-name]** hierarchy level, the verify source address function does not work in the uplink direction. [PR/807402]

#### **Charging**

- Even after multiple changes in aggregated maximum bit rate (AMBR) uplink or downlink, no charging data record (CDR) is generated until session deletion. [PR/806453]
- A charging trigger with aggregated multiservice PIC (**ams**) high-availability switchover causes generation of an addition CDR with **causeForRecordClosing:managementIntervention**. [PR/806414]

#### **Dedicated Bearer QoS**

If network-initiated dedicated bearer (secondary PDP context) activations fail due to reaching the configured anchor Packet Forwarding Engine (APFE) maximum bearers limit, then the P-GW does not increment the **APFE Resource Unavailable** statistics. [PR/795717]

### **GTP**

During GTPv1 to GTPv2 handover, the S-GW sends P-GW control and data tunnel endpoint identifiers (TEIDs) in the Create Session response. These TEIDs should not be sent. [PR/802575]

### **GTP QoS**

- As part of the Serving GPRS Support Node (SGSN) change event reporting, if a Credit Control Answer - Update (CCA-U) message from the policy charging rules function (PCRF) contains a Charging-Rule-Install for the primary Packet Data Protocol (PDP) context (bearer) along with new quality-of-service (QoS) values for the primary PDP, then the Packet Data Network Gateway (P-GW) sends an Update PDP Request with the QoS Information Element (IE) set to all zeros (0). This value should reflect the QoS values in the received CCA-U. [PR/795627]
- During the lifetime of a GPRS Tunneling Protocol version 1 (GTPv1) session, if the PCRF sends a Reauthorization Request (RAR) with the QoS change (different AMBR or QCI), then the P-GW sends an Update PDP Request with MBR values set to 0 in the QoS IE. These values should reflect the values received in the RAR. [PR/803592]
- If you configure a basic GTPv1 configuration for an APN without Gx configuration, the GTPv2 mapped values for PVI and PCI are set incorrectly to 1. The allocation retention priority (ARP) mapping is correct. [PR/806867]

### **Inline Reassembly**

If you configure the inline reassembly feature as a service set and then issue the **show services inline ip-reassembly statistics** command for the Flexible PIC Concentrator (FPC), Packet Forwarding Engine, or service interface configured for inline IP reassembly, then the value in the **Total fragments punted to UPIC** field actually represents the total number of fragments dropped due to low memory detection. [PR/805037]

### **PCEF**

For dynamic policies, when GTPv1 to GTPv2 handover occurs, and you issue the **show unified-edge ggsn-pgw subscribers extensive** command, the uplink and downlink GBR values are set to zero (0) and the uplink and downlink maximum bit rate (MBR) values are incorrect. [PR/801706]

## **Previous Software Release**

### **Outstanding Issues in Junos OS Release 12.1WB2 for the MobileNext Broadband Gateway**

---

#### **Chassis**

- During periods of high subscriber creation and deletion and multiple graceful Routing Engine switchovers (GRES), the output of the **show unified-edge ggsn-pgw statistics** command can sometimes display negative values in the **Gateway initiated sessions deactivations** and **Successful gateway initiated deactivation** fields. [PR/773468]
- When deleting subscribers at a high rate, a session PIC switchover causes some subscriber deletions not to reach the services PIC, and subscribers can still appear on

the services PIC although they have been deleted on the session PIC. This occurs when the same services PIC is serving two session PICs. [PR/773462]

### ***GTP***

In some cases, after you issue a **clear unified-edge sgw statistics gateway gateway-name** command, GTP statistics for a previous session are not cleared. As a workaround, issue a show command such as **show unified-edge sgw gtp statistics gateway gateway-name**, and then issue the **clear unified-edge sgw statistics gateway gateway-name** command. [PR/724619]

### ***IP Address Pool***

Duplicate IP address allocation is not checked for conflicts between local-pool and network-behind-mobile prefixes. You must configure a non-overlapping local pool and network-behind-mobile prefix pool. [PR/720085]

### ***IPsec and NAT Services***

Configuration changes and deletions to NAT services do not work when the system is running. [PR/610284]

### ***IPsec and Services***

We recommend that you configure a **policy-db-size** value of at least 1024 at the **[edit chassis fpc fpc-number pic pic-number adaptive-services service-package extension-provider]** hierarchy level. [PR/663332]

### ***QoS/CAC***

Wildcard configuration for mobile interfaces (**mif-**) is not supported at the **[edit class-of-service]** hierarchy level. Therefore, DiffServ code point (DSCP) ingress rewrite and egress classification do not apply to mobile interfaces when wildcards are used. As a workaround, use the specific mobile interface values instead of a wildcard configuration. [PR/577828]

## Errata in Junos OS Release 12.1W for MobileNext Broadband Gateway Documentation

The documentation errors for the MobileNext Broadband Gateway are as follows:

- The command **request unified-edge ggsn-pgw call-trace start imsi *imsi-number*** has an undocumented ***file-name-prefix*** parameter. The *file-name-prefix* entered is prepended to the call trace file, along with user name and timestamp (separated by underscores). You can examine the value prepended with the **request unified-edge ggsn-pgw call-trace show** command.

## General Information

---

### Requesting Technical Support

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

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

### Self-Help Online Tools and Resources

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

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

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

## Opening a Case with JTAC

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

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

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

## Copyrights

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

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

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