

Junos[®] OS Release 12.1W2 MobileNext Broadband Gateway Release Notes

Release 12.1W2
1 April 2013
Revision 1

These release notes accompany Release 12.1W2 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 12.1W2 for the MobileNext Broadband Gateway	3
Diameter	3
Policy and Charging Enforcement Function	5
Charging	6
Changes in Default Behavior in Junos OS Release 12.1W2 for the MobileNext Broadband Gateway	9
Resolved Issues in Junos OS Release 12.1W2 for the MobileNext Broadband Gateway	10
APNs	10
Chassis	11
Charging	11
Dedicated Bearer QoS	11
GTP	11
GTP QoS	11
PCEF	12
QoS/CAC	12

Issues in Junos OS Release 12.1W2 for the MobileNext Broadband Gateway	12
Current Software Release	12
Outstanding Issues in Junos OS Release 12.1W2 for the MobileNext Broadband Gateway	12
Previous Software Release	14
Outstanding Issues in Junos OS Release 12.1W for the MobileNext Broadband Gateway	14
Changes to and Errata in Documentation for Junos OS Release 12.1W2 for the MobileNext Broadband Gateway	15
Changes to the Documentation	15
Errata	16
Upgrade and Downgrade Instructions for Junos OS Release 12.1W for the MobileNext Broadband Gateway	16
Before You Upgrade Software Releases	16
Planning Considerations for the Upgrade	17
Preparing for the Upgrade	17
Backing Up the Current Installation	18
Downloading the Software	19
Upgrading a Router with Redundant Routing Engines to Release 12.1W	19
Verifying the Upgrade	23
Downgrading the Software	24
General Information	26
Requesting Technical Support	26
Self-Help Online Tools and Resources	26
Opening a Case with JTAC	26
Copyrights	27

New Features in Junos OS Release 12.1W2 for the MobileNext Broadband Gateway

The following features have been added to Junos OS Release 12.1W2 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. The Diameter profiles can also be used to exclude or include Diameter attribute-value pairs (AVPs) in the Credit Control Request (CCR) messages between the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW) and the Online Charging System (OCS) or the Policy and Charging Enforcement Function (PCEF).

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.

To configure the AVPs excluded or included in the CCR messages, include the **attributes exclude** and **attributes include** statements at the **[edit unified-edge diameter-profiles gy-profile profile-name]** or **[edit unified-edge diameter-profiles gx-profile profile-name]** hierarchy level.



NOTE: Although the following configuration statements are visible on the router, they are not fully supported in the current release. Therefore, we recommend that you do not configure these statements.

- The **gx-capability-list** and **rule-suggestion** statements at the **[edit unified-edge diameter-profiles gx-profile profile-name attributes include]** hierarchy level.
- The **cumulative-used-service-unit**, **credit-instance-id**, and **service-start-timestamp** statements at the **[edit unified-edge diameter-profiles gy-profile profile-name attributes include]** hierarchy level.

[MobileNext Broadband Gateway Configuration Guide]

Policy and Charging Enforcement Function

- **Support for application-aware PCC rules (Broadband Gateway MX Series platforms)**—You can configure application-aware PCC rules that use deep packet inspection (DPI) to support policies for Layer 7 and higher-layer application traffic. An application-aware PCC rule can specify applications, application groups, and nested applications as match conditions for filtering subscriber traffic and assigning the appropriate quality of service (QoS), charging, and gating controls for that traffic. The applications, application groups, and nested applications specified in PCC rules are either predefined Junos OS application signatures or custom application signatures that you configure from the application identification (APPID) feature.

To enforce application-aware PCC rules, the policy and charging enforcement function (PCEF) is applied as a service on the APN (MIF interface) to indicate to the Packet Forwarding Engine that traffic should be directed to the Junos OS services PIC that hosts the PCEF service. When subscriber traffic is redirected to the services PIC, processing is completed and the appropriate policies are applied as a service on the MIF interface associated with an APN. To enforce Layer 3 and Layer 4 PCC rules, the Packet Forwarding Engine inspects uplink and downlink subscriber traffic on an access point name (APN).



NOTE: For application-aware PCC rules, the PCRF can only refer PCC rules or rulebases (static Gx policies) that are statically configured on the MobileNext Broadband Gateway.

[*MobileNext Broadband Gateway Configuration Guide*]

- **Support for failure handling when the PCRF goes down (Broadband Gateway MX Series platforms)**—You can configure parameters to determine the action that the broadband gateway performs when the PCRF goes down by specifying one of the following failure-action statements at the `[edit unified-edge pcef profiles profile-name dynamic-policy-control failure-handling]` hierarchy level:
 - To continue the existing Gx session with the dynamic rules and rulebases (if the rules are present) and prevent the PCEF from making any retry attempts, configure the **failure-action continue** statement.
 - To continue the existing Gx session and prompt the PCEF to attempt to reconnect with the PCRF, configure the **failure-action continue-and-retry** statement.
 - To terminate the existing session and start a new session by applying the rule or rulebase that is configured in the failure-handling container in the PCEF profile, configure the **failure-action terminate** statement.



NOTE: Although the **failure-action**, **pcc-rulebases**, and **pcc-rules** configuration statements (at the `[edit unified-edge pcef profiles profile-name dynamic-policy-control failure-handling]` hierarchy level) are visible on the router, they are not fully supported in the current release. Therefore, we recommend that you do not configure these statements.

[MobileNext Broadband Gateway Configuration Guide]

- **Support for session failover (Broadband Gateway MX Series platforms)**—To specify that online charging sessions should not fail over to an alternate server, configure the **session-failover-not-supported** statement at the **[edit unified-edge pcef profiles profile-name dynamic-policy-control]** hierarchy level. The failover of online charging sessions to an alternate server is enabled by default.

[MobileNext Broadband Gateway Configuration Guide]

- **Support for Release 8 or Release 9 attribute-value pairs (AVPs) compliance (Broadband Gateway MX Series platforms)**—You can configure the release (Release 8 or Release 9) that the Gx interface uses at the PDN gateway (P-GW) so that the P-GW will receive only the AVPs compliant to the configured release version. You configure release compliance for AVPs by configuring the **release [r8 | r9]** statement at the **[edit unified-edge pcef profiles profile-name dynamic-policy-control]** hierarchy level. When the **r8** option is configured, the P-GW sends one Supported-Features AVP for release 8 marked as Mandatory, ignores the Supported-Features AVP in the PCRF response, and behaves according to Release 8. When the **r9** option is configured, the P-GW sends two Supported Features AVPs, one each for release 8 and release 9 responses, and both are marked as Mandatory. The P-GW ignores the Supported-Features AVP in the PCRF response, and behaves according to Release 9.

[MobileNext Broadband Gateway Configuration Guide]

Charging

- **Support for advice of charge and top-up (Broadband Gateway MX Series platforms)**—You can configure the broadband gateway to provide support for advice of charge (AoC) and top-up. The AoC feature provides a subscriber with information about any applicable charges when the subscriber uses a service. AoC information is provided before the subscriber uses the service, and the subscriber must accept the charges in order to use the service. The charges are applied in real time until the subscriber's quota is exhausted. The subscriber is then given the opportunity to recharge; this is called top-up.

To enable support for AoC and top-up on the broadband gateway, you must configure the policy and charging enforcement function (PCEF) parameters for a service set. In addition, you must configure the AoC input and output service filters and apply the filters to the mobile interface of the access point name (APN).

[MobileNext Broadband Gateway Configuration Guide]

- **Support for specifying the node identifier format in subscriber CDRs (Broadband Gateway MX Series platforms)**—On the broadband gateway, you can specify the format of the node identifier that is included in the charging data records (CDRs) of subscribers. The node identifier indicates the node that generated the CDR.

To specify the format of the node identifier included in subscriber CDRs, include the **node-id** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging cdr-profiles profile-name]** hierarchy level.

[MobileNext Broadband Gateway Configuration Guide]

- **Including the requested APN in subscriber CDRs (Broadband Gateway MX Series platforms)**—You can configure the broadband gateway to include the requested APN in CDRs of subscribers attached to a CDR profile. Therefore, when the APN type is virtual, the broadband gateway includes the requested or virtual APN in the CDRs.

To configure the inclusion of the requested APN in CDRs, include the **report-requested-apn** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging cdr-profiles profile-name]** hierarchy level.

[MobileNext Broadband Gateway Configuration Guide]

- **Reporting both active and inactive rating groups on bearer termination (Broadband Gateway MX Series platforms)**—You can configure the broadband gateway to report both active and inactive rating groups on bearer termination. The broadband gateway then returns the quota that it receives preemptively from the Online Charging System (OCS) when a bearer is terminated.

To configure the reporting of both active and inactive rating groups on bearer termination, include the **all-rgs-on-termination** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging transport-profiles profile-name online]** hierarchy level.

[MobileNext Broadband Gateway Configuration Guide]

- **Excluding MSCC AVPs from CCR-T messages to the OCS (Broadband Gateway MX Series platforms)**—You can configure the broadband gateway to exclude Multiple Services Credit Control (MSCC) attribute-value pairs (AVPs) from Credit Control Request Terminate (CCR-T) messages sent to the OCS. This configuration is useful in cases where the OCS does not support the MSCC AVP in CCR-T messages.

To configure the exclusion of MSCC AVPs from CCR-T messages to the OCS, include the **no-mscc-in-ccrt** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging transport-profiles profile-name online]** hierarchy level.



NOTE: Although the **no-mscc-in-ccrt** statement is visible on the router, it is not fully supported in the current release. Therefore, we recommend that you do not configure this statement.

[MobileNext Broadband Gateway Configuration Guide]

- **Requesting quota from the OCS only on receipt of the first packet for a rating group (Broadband Gateway MX Series platforms)**—You can configure the broadband gateway to request quota (for a rating group) from the OCS only on receipt of the first packet matching that rating group. This configuration is valid at the rating group level.

To configure the requesting of quota from the OCS only on receipt of the first packet for a rating group, include the **quota-request-on-first-packet** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging transport-profiles profile-name online]** hierarchy level.

[MobileNext Broadband Gateway Configuration Guide]

- **Sending a CCR-I message only on receipt of the first packet for any rating group of a bearer (Broadband Gateway MX Series platforms)**—You can configure the broadband gateway to send a CCR-Initial (CCR-I) message to the OCS only on receipt of the first packet for any rating group of the bearer. This configuration is valid at the bearer level.

To configure the sending of a CCR-I message only on receipt of the first packet for any rating group of the bearer, include the **send-ccri-on-first-packet** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging transport-profiles profile-name online]** hierarchy level.



NOTE: Although the **send-ccri-on-first-packet** statement is visible on the router, it is not fully supported in the current release. Therefore, we recommend that you do not configure this statement.

[MobileNext Broadband Gateway Configuration Guide]

- **Including a single MSCC AVP in CCR-T messages (Broadband Gateway MX Series platforms)**—You can configure the broadband gateway to include only one MSCC AVP in CCR-T messages sent to the OCS. This configuration is useful in cases where the OCS supports only one MSCC AVP in CCR-T messages.

To configure the inclusion of a single MSCC AVP in CCR-T messages to the OCS, include the **single-mscc-in-ccrt** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging transport-profiles profile-name online]** hierarchy level.



NOTE: Although the **single-mscc-in-ccrt** statement is visible on the router, it is not fully supported in the current release. Therefore, we recommend that you do not configure this statement.

[MobileNext Broadband Gateway Configuration Guide]

- **Support for quota holding time (Broadband Gateway MX Series platforms)**—You can configure quota holding time on the broadband gateway. The quota holding time indicates the number of seconds for which the quota granted by the OCS is held by the gateway when no traffic is received for that rating group. The configured quota holding time is used if the OCS does not provide a quota holding time in the Quota-Holding-Time AVP in the Credit Control Answer (CCA) message.

To configure the quota holding time on the broadband gateway, include the **quota-holding-time** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name online]** hierarchy level.



NOTE: Although the **quota-holding-time** statement is visible on the router, it is not fully supported in the current release. Therefore, we recommend that you do not configure this statement.

[MobileNext Broadband Gateway Configuration Guide]

- **Support for always including the RSU AVP in CCR messages to the OCS (Broadband Gateway MX Series platforms)**—You can configure the broadband gateway to always include the Requested-Service-Unit (RSU) AVP in CCR messages to the OCS.

To configure support for always including the RSU AVP on the broadband gateway, include the **always-include** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name online requested-service-unit]** hierarchy level.

[MobileNext Broadband Gateway Configuration Guide]

- **Support for including the RSU AVP in CCR messages when the quota holding time elapses (Broadband Gateway MX Series platforms)**—You can configure the broadband gateway to include the RSU AVP in CCR messages to the OCS when usage is reported for the reason of quota holding time, that is, when the quota holding time elapses.

To configure support for including the RSU AVP when the quota holding time elapses, include the **include-quota-holding-time** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging trigger-profiles profile-name online requested-service-unit]** hierarchy level.

[MobileNext Broadband Gateway Configuration Guide]

Changes in Default Behavior in Junos OS Release 12.1W2 for the MobileNext Broadband Gateway

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

- The lower limit for the **maximum-bearers** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name apn-services apns apn-name]** hierarchy level has been changed from 100,000 to 1000. [PR/692887]

[MobileNext Broadband Gateway Statements and Commands Reference Guide]

- The lower limit for the **maximum-bandwidth** statement at the **[edit unified-edge cos-cac gbr-bandwidth-pools name]** hierarchy level has been changed from 50,000 to 1000. [PR/692887]

[MobileNext Broadband Gateway Statements and Commands Reference Guide]

- In IPv4 mobile address pools, used for externally assigned or gateway assigned addresses, only the network address and the broadcast address are blocked from being assigned to subscribers. Previously, all addresses in the mobile address pool ending with 0 or 255 were blocked from being assigned to subscribers. [PR/729144]

[MobileNext Broadband Gateway Configuration Guide]

- If user closed subscriber group (CSG) based charging is enabled for a P-GW or S-GW subscriber, then the user CSG information is displayed in the output of the **show unified-edge ggsn-pgw subscribers** or **show unified-edge sgw subscribers** commands. [PR/800184]

[MobileNext Broadband Gateway Statements and Commands Reference Guide]

- The **brief** and **detail** options have been added to the **show unified-edge ggsn-pgw diameter peer status** command. [PR/814325]
[MobileNext Broadband Gateway Statements and Commands Reference Guide]
- The **diameter-avp-profiles** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name charging]** hierarchy level has been deprecated. In addition, the attribute-value pairs (AVPs) that can be excluded from Credit Control Request (CCR) messages have been moved from the **[edit unified-edge gateways ggsn-pgw gateway-name charging diameter-avp-profiles profile-name exclude-avp-options]** hierarchy level to the **[edit unified-edge diameter-profiles gy-profile profile-name attributes exclude]** hierarchy level. [PR/817602]
[MobileNext Broadband Gateway Statements and Commands Reference Guide]
- If usage monitoring is enabled for a session, the output of the **show unified-edge ggsn-pgw subscribers** command displays the usage monitoring information. [PR/821430]
[MobileNext Broadband Gateway Statements and Commands Reference Guide]
- The attribute number of the Redirect-Gw-Addr vendor-specific attribute (VSA) has been changed to VSA 26-175, and the attribute number of the APN-Name VSA has been changed to VSA 26-176. [PR/828734]
[MobileNext Broadband Gateway Configuration Guide]
- The **capabilities-exchange-timeout** statement has been moved from the **[edit access diameter peer peer-name]** hierarchy level to the **[edit access diameter peer peer-name connect-actively]** hierarchy level. In addition, the **connection-repeat-timeout**, **connection-retry-timeout**, and **connection-timeout** statements at the **[edit access diameter peer peer-name]** hierarchy level have been moved to the **[edit access diameter peer peer-name connect-actively]** hierarchy level and renamed to **repeat-timeout**, **retry-timeout**, and **timeout**, respectively. [PR/845593]
[MobileNext Broadband Gateway Statements and Commands Reference Guide]
- The lower limit for the **charging-characteristics** statement at the **[edit unified-edge gateways ggsn-pgw gateway-name service-selection-profiles profile-name term name from]** hierarchy level has been changed from 1 to 0. [PR/858415]
[MobileNext Broadband Gateway Configuration Guide]
[MobileNext Broadband Gateway Statements and Commands Reference Guide]

Resolved Issues in Junos OS Release 12.1W2 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.

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]

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]

Charging

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

Dedicated Bearer QoS

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

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]
- 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]

PCEF

For dynamic polices, 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]

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]

Issues in Junos OS Release 12.1W2 for the MobileNext Broadband Gateway

The current software release is Release 12.1W2 for the MobileNext Broadband Gateway.

- [Current Software Release on page 12](#)
- [Previous Software Release on page 14](#)

Current Software Release

Outstanding Issues in Junos OS Release 12.1W2 for the MobileNext Broadband Gateway

Charging

- A charging SNMP MIB walk generates a core file in the mobile daemon (mobiled) when:
 - The maximum number of charging transport profiles or the maximum number of GTP Prime (GTPP) peer profiles is configured. There is no workaround. Do not query the charging MIB when the maximum number of charging transport profiles or the maximum number of GTPP peer profiles is configured.
 - Existing charging transport profiles are deleted and new charging transport profiles are added more than once in the same configuration commit. As a workaround, delete the existing charging transport profiles in one configuration commit, and add the new charging transport profiles in the next configuration commit, and then continue with the charging SNMP MIB walk.

- Existing GTPP peer profiles are deleted and new GTPP peer profiles are added more than once in the same configuration commit. As a workaround, delete the existing GTPP peer profiles in one configuration commit, and add the new GTPP peer profiles in the next configuration commit, and then continue with the charging SNMP MIB walk.

[PR/860721]

Chassis

- If graceful Routing Engine switchover occurs twice on the broadband gateway, some session PICs are not displayed as part of the resource manager clients when you run the **show unified-edge ggsn-pgw resource-manager clients** command. [PR/807735]
- When the primary session PIC is restarted, it becomes the secondary session PIC once it comes back online. The subscribers are now backed up on the secondary PIC. However, all the subscribers are not synchronized from the primary to the secondary and the sync state is displayed as "In progress." [PR/844513]
- When an active services PIC goes down and the new active services PIC, which replaces the previous active services PIC, also goes down, the subscriber's bearer state is stuck in cleanup mode. [PR/846744]
- When graceful Routing Engine switchover occurs because of kernel panic, the primary session PIC is stuck in the "Connecting" state. [PR/847777]
- When the chassis on a co-located gateway is rebooted, the resource manager clients (Packet Forwarding Engines, session PICs, and services PICs) do not come up. [PR/852700]
- After graceful Routing Engine switchover, the backup services PIC is not displayed as part of the resource manager clients when you run the **show unified-edge ggsn-pgw resource-manager clients** command. [PR/853933]

Deep Packet Inspection (DPI)

- When there are changes in the configuration of PCC rules (at the **[edit unified-edge pcef pcc-rules]** hierarchy level), in some cases the configuration changes are not updated correctly, resulting in unknown behaviors including packet drops. As a workaround, reboot the services PICs when you make configuration changes to PCC rules. [PR/835721]
- The broadband gateway does not count some uplink packets for subscribers with DPI and HTTP header enrichment. [PR/837733]
- In the current service chain, the HTTP header enrichment plug-in is called before the PCEF plug-in. This leads to extra bytes being counted because the HTTP header enrichment plug-in inserts tags in the HTTP header. [PR/837739]
- The number of uplink and downlink packets displayed in the output of the **show unified-edge ggsn-pgw subscribers extensive** and **show unified-edge ggsn-pgw subscribers charging extensive** commands is incorrect. [PR/844436]
- On co-located gateways, if a session PIC switchover occurs when subscribers are being deleted, then a few subscribers on the services PIC are not deleted. Therefore, some

subscribers still appear on the services PIC although they have been deleted on the session PIC. As a workaround, reboot the services PIC. [PR/858272]

- If you modify the PCEF configuration on co-located gateways, the **show unified-edge ggsn-pgw status command** does not work. As a workaround, reboot the services PIC when you modify the PCEF configuration. [PR/859106]

GTP

- If the Cisco Serving GPRS Support Node (SGSN) interoperating with the broadband gateway (GGSN) initiates the creation of a Direct Tunnel (DT) enabled primary PDP context, and if the PCRF initiates the creation of a secondary PDP context tailgating the creation of the primary PDP context, then both the primary and the secondary PDP contexts are not created. [PR/828680]
- The Serving Gateway (S-GW) ignores the indication from the GTP peer that the GTP version is not supported and keeps sending GTPv2 messages back to the GTP peer. [PR/854707]

PCEF

- Subscribers for whom Modify Bearer Requests are sent are stuck in the “wait” state if the Layer 7 rating group has the highest precedence. This issue can occur if signaling triggers are enabled and if both Layer 3 and Layer 7 rules are used, with Layer 7 rules having a higher precedence. As a workaround, exclude signaling triggers or configure Layer 3 rules with the highest precedence; if Layer 7 rules must be given higher precedence among all valid Layer 3 and Layer 7 rules, then configure a dummy Layer 3 rule with the highest precedence. [PR/860466]

QoS

- Maintenance mode is not supported for changing the configuration of guaranteed bit rate (GBR) bandwidth pools at the **[edit unified-edge cos-cac gbr-bandwidth-pools name]** hierarchy level. As a workaround, before modifying the configuration of a GBR pool, ensure that there are no subscribers (on all configured gateways) referencing that GBR bandwidth pool. If the GBR bandwidth pool configuration is changed when there are subscribers referencing that GBR bandwidth pool, some subscriber services may be affected for GBR and dedicated bearers. [PR/851910]

Previous Software Release

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

Chassis

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]

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]

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]

Changes to and Errata in Documentation for Junos OS Release 12.1W2 for the MobileNext Broadband Gateway

- [Changes to the Documentation on page 15](#)
- [Errata on page 16](#)

Changes to the Documentation

The following are the changes made to the documentation:

- The *MobileNext Broadband Gateway Configuration Guide* has been divided into three documents:
 - *Configuration Guide*
 - *Statements and Commands Reference Guide*
 - *Monitoring and Troubleshooting Guide*
- The format of the Framed-Route and Framed-IPv6-Route AVPs that must be configured on the RADIUS server for obtaining network-behind-mobile prefixes from the RADIUS server is now documented. This information was not present in the documentation for the previous release.
- If the RADIUS server is used to assign IP addresses to subscribers on the broadband gateway, the information about the AVPs (Framed-IP-Address or Framed-IPv6-Prefix) that must be configured on the RADIUS server is now documented. This information was not present in the documentation for the previous release.

Errata

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

- The AAA framework uses vendor ID 4874, which is assigned to Juniper Networks by the Internet Assigned Numbers Authority (IANA).

[MobileNext Broadband Gateway Configuration Guide]

- Although it is not documented, you can configure a merged S11 (to an MME) and S4 (to an SGSN) interface for a S-GW GTP peer. The merged S11-S4 interface uses one IP address and avoids handover issues when the S11 and S4 interface GTP peers have different IP addresses. For example, you can configure a **s11-s4** GTP peer at the **[edit unified-edge sgw sgw-name gtp peer]** hierarchy level. [PR/751002]

[MobileNext Broadband Gateway Configuration Guide]

Upgrade and Downgrade Instructions for Junos OS Release 12.1W for the MobileNext Broadband Gateway

This section discusses the following topics:

- [Before You Upgrade Software Releases on page 16](#)
- [Upgrading a Router with Redundant Routing Engines to Release 12.1W on page 19](#)
- [Verifying the Upgrade on page 23](#)
- [Downgrading the Software on page 24](#)

Before You Upgrade Software Releases

To upgrade to Junos OS Release 12.1W or later, you must be running Junos OS Release 11.4W2 or later versions.



WARNING: If you are upgrading from Release 11.4W1 and earlier to Release 11.4W2 and later, contact your Juniper Networks support representative before trying to upgrade.

Before you start the upgrade, we recommend you have the following items available:

- MobileNext Broadband Gateway product documentation
- A console port connection to the Routing Engines (optional)
- **jinstall64** and **jmobile** packages for the current software releases for fallback purposes
- **jinstall64** and **jmobile** packages for the new software releases



NOTE: You cannot upgrade or downgrade more than three releases.

Planning Considerations for the Upgrade

A software upgrade for MobileNext Broadband Gateway in a live network impacts network traffic. You should upgrade the software at a time when the load on the MobileNext Broadband Gateway is at its lowest. For a redundant Routing Engine configuration, the downtime is approximately 5 to 6 minutes, during which the broadband gateway is unavailable for traffic.

If APNs handled by the broadband gateway being upgraded can be redundantly handled by other broadband gateways in the network, we recommend that new traffic be redirected to the redundant broadband gateways by changing the entries in the core DNS nodes. Once the new traffic is redirected, reduce the traffic in the broadband gateway that is being upgraded to a minimum.

Preparing for the Upgrade

Before you upgrade, verify the health of the MobileNext Broadband Gateway and resolve any issues or alarms. Record the command output for later comparison.

To prepare for the upgrade, execute these commands on the current master Routing Engine. In this case, re0 is the master Routing Engine.



NOTE: Although the steps show both **ggsn-pgw** and **sgw** commands, you only need to run the commands for the corresponding configured gateway.

To prepare for the upgrade:

1. Verify the current Routing Engine redundancy state.

```
re0> show chassis routing-engine
```

2. Verify the loaded software version.

```
re0> show version
```

3. Display the maintenance mode status of the broadband gateway.

```
re0> show unified-edge ggsn-pgw service-mode
re0> show unified-edge sgw service-mode
```

4. Display the operational status of the broadband gateway.

```
re0> show unified-edge ggsn-pgw status detail
re0> show unified-edge sgw status detail
```

5. Display the status of the system interfaces for the broadband gateway.

```
re0> show unified-edge ggsn-pgw system interfaces
re0> show unified-edge sgw system interfaces
```

6. Display the chassis alarms.

```
re0> show chassis alarms
```

7. Display the system alarms.

re0> show system alarms

8. Display the status for the installed FPCs.

re0> show chassis fpc detail

9. Display the status for the PICs.

re0> show chassis fpc pic-status

10. Display summary information for the interfaces and display the status of the mobile interfaces for all APNs.

re0> show interfaces terse

re0> monitor interface mif.*unit*

where *unit* is the mobile interface unit for the APN to be monitored.

11. Display statistics for the broadband gateway.

re0> show unified-edge ggsn-pgw statistics

re0> show unified-edge sgw statistics

12. Display statistics for all APNs.

re0> show unified-edge ggsn-pgw apn statistics apn-name *apn-name*

13. Review system log messages.

re0> show log messages | last 150 | no-more

14. Display the disk space on the broadband gateway.

re0> show system storage

re0> request routing-engine login other-routing-engine

re1> show system storage

re1> exit

15. Display graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) synchronization status.

re0> show task replication

Backing Up the Current Installation

Before upgrading, back up the file system and the currently active Junos OS configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. Issue the following command:

user@host> request system snapshot routing-engine both

When this command is issued, the `/root` and `/config` file system on the router's CompactFlash card are backed up to the `/altroot` and `/altconfig` file systems on the router's hard disk. When the backup is completed, the current and backup software installations are identical.



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software because the running copy and the backup copy of the software are identical.

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts might be removed. Files that are retained are the **juniper.conf** and **ssh** files, scripts in official locations, and CDR files. To preserve the stored files, copy them to another system before upgrading or downgrading the MobileNext Broadband Gateway.

Downloading the Software

The download and installation process for Junos OS MobileNext Broadband Gateway releases is different from Junos OS releases. To download the software:

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks web page at <http://www.juniper.net/support/downloads/>.
2. Select **MobileNext Broadband Gateway** under Mobility for the software that you want to download.
3. Select the type (Junos US/Canada or Junos Worldwide) from the **Type** drop-down list to the right of the Download Software page.
4. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.
5. Select the **Software** tab.
6. In the **Install Package & Media** section of the **Software** tab, select the software packages (64-bit Junos Install Package and Junos MobileNext Routing Engine Software) for the release.
7. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
8. Review and accept the End User License Agreement.
9. Download the software to a local host.
10. Copy the software to the routing platform or to your internal software distribution site.

Upgrading a Router with Redundant Routing Engines to Release 12.1W

When upgrading or downgrading Junos OS, always use the **jinstall** package. You must also use the **jmobile** package to enable MobileNext Broadband Gateway on the MX Series router.



NOTE: The **jinstall** and **jmobile** packages that you download must be for the same release; for example, **jinstall64-12.1W1-domestic-signed.tgz** and **jmobile-12.1W1-signed.tgz**.

The domestic type (for US/Canada) includes high-encryption capabilities for data leaving the router, while the export type (for Worldwide) does not.

Follow this procedure to upgrade the broadband gateway configured with redundant Routing Engines. In this procedure, re0 is the master Routing Engine and re1 is the backup Routing Engine.



NOTE: We recommend that you upgrade all software packages out of band using the console because in-band connections are lost during the upgrade process.

To upgrade the broadband gateway:

1. Make sure there is enough free storage space on the broadband gateway (`/var` directory) for the upgrade. We recommend that you have at least three times the software size available after the files have been copied to the Routing Engine.

re0> show system storage detail

- a. Verify there is enough storage space on the other Routing Engine.

re0> request routing-engine login other-routing-engine

re1> show system storage

re1> exit

- b. List old installation packages and core dumps. Delete them and other such files that are no longer needed.

re0> file list /var/tmp

re0> show system core-dumps

re0> file delete *filename*

- c. Clean up temporary files and rotate logs.

re0> request system storage cleanup dry-run

re0> request system storage cleanup

2. Copy the new Junos OS package and mobility package that were downloaded (see [“Downloading the Software” on page 19](#)) from `/var/tmp` on re0 to re1. For example, `jinstall64-12.1W1-export-signed.tgz` and `jmobile-12.1W1-signed.tgz` were downloaded.

re0> file copy /var/tmp/jinstall64-12.1W1-export-signed.tgz re1:/var/tmp

re0> file copy /var/tmp/jmobile-12.1W1-signed.tgz re1:/var/tmp

3. (Optional) If new requests to the broadband gateway should be rejected so that they are redirected to another gateway, set the broadband gateway to maintenance mode.

re0> configure

re0# set unified-edge gateways ggsn-pgw *gateway name* service-mode maintenance

re0# set unified-edge gateways sgw *gateway name* service-mode maintenance

re0# commit synchronize

re0# exit

4. (Optional) If you must upgrade without subscribers, clear the subscribers.

re0> clear unified-edge ggsn-pgw subscribers *gateway gateway name*

re0> clear unified-edge sgw subscribers *gateway gateway name*

Wait for 3 minutes and then verify the number of subscribers.

re0> show unified-edge ggsn-pgw status session-state detail

```
re0> show unified-edge sgw status session-state detail
```

If the number of subscribers is not yet 0, wait for 3 more minutes and repeat the **show** command to verify whether the number of subscribers is decreasing. If the number is greater than 0, repeat the **clear** command. If the subscribers are still not cleared, use the **force** option with the **clear** command.

5. Disable NSR and GRES and save the configuration change to both Routing Engines.

```
re0> configure
re0# deactivate routing-options nonstop-routing
re0# deactivate chassis redundancy graceful-switchover
re0# commit synchronize and-quit
```

6. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.

```
re0> request routing-engine login other-routing-engine
re1> request system software add /var/tmp/jinstall64-12.1W1-export-signed.tgz
validate reboot
```



NOTE: The **validate** option validates the software package against the current configuration as a prerequisite to adding the software package, to ensure that the router reboots successfully. This is the default behavior when the software package being added is a different release.

Adding the **reboot** option reboots the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process can take 5 to 10 minutes. Rebooting occurs only if the upgrade is successful.

For a redundant Routing Engine configuration, only the backup Routing Engine is rebooted. The active Routing Engine stays up and there is no downtime. To return to the previously installed software, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

7. Wait for the backup Routing Engine to finish rebooting. Repeat the following command until the Routing Engine is back up, which should take around 5 minutes.

```
re0> show chassis routing-engine
```

Log in to the backup Routing Engine and verify that the new software is loaded.

```
re0> request routing-engine login other-routing-engine
re1> show version
```

8. Install the mobility release on the backup Routing Engine.

```
re1> request system software add /var/tmp/jmobile-12.1W1-signed.tgz validate reboot
```



NOTE: Adding the **reboot** option reboots the router after the upgrade is validated and installed. The loading process takes about 2 minutes. Rebooting occurs only if the upgrade is successful.

9. Wait for the backup Routing Engine to finish rebooting. Repeat the following command until the Routing Engine is back up, which should take around 3 minutes.

```
re0> show chassis routing-engine
```

Log in to the backup Routing Engine and verify that the new software is loaded.

```
re0> request routing-engine login other-routing-engine
re1> show version
```

10. Transfer routing control to the backup Routing Engine to activate the new software.

```
re1> exit
re0> request chassis routing-engine master switch
```



NOTE: This process takes about 6 minutes. The command activates the new software and causes the session PICs and PFEs to be reset when the new Routing Engine takes over. The session PIC and PFE states are rebuilt as soon as they are back online as RMPsD clients. PDP sessions or bearers are not able to transfer data and new activations (as well as any GTP-C procedures) are not processed during this time.

After the switch, re0 becomes the backup Routing Engine and re1 (with the new software) becomes the master Routing Engine.

Make sure that the new software is running correctly by following the steps in [“Verifying the Upgrade” on page 23](#).



NOTE: If the system functions poorly at this point, you can easily return to the previously installed software by transferring routing control back to the Routing Engine running the old configuration.

11. Install the software release on the new backup Routing Engine and reboot. Only the backup Routing Engine is rebooted. The active Routing Engine stays up and there is no downtime.

```
re1> request routing-engine login other-routing-engine
re0> show version
re0> request system software add /var/tmp/jinstall64-12.1W1-export-signed.tgz
validate reboot
```



NOTE: To return to the previously installed software, you must issue the `request system software add validate` command and specify the `jinstall` package that corresponds to the previously installed software.

12. Wait for the new backup Routing Engine to finish rebooting. Repeat the following command until the Routing Engine is back up, which should take around 5 minutes.

```
re1> show chassis routing-engine
```

Log in to the backup Routing Engine and verify that the new software is loaded.

```
re1> request routing-engine login other-routing-engine
re0> show version
```

13. Install the mobility package on the new backup Routing Engine and reboot.

```
re0> request system software add /var/tmp/jmobile-12.1W1-signed.tgz validate reboot
```

14. Wait for the backup Routing Engine to finish rebooting. Repeat the following command until the Routing Engine is back up, which should take around 3 minutes.

```
re1> show chassis routing-engine
```

Log in to the backup Routing Engine and verify that the new software is loaded.

```
re1> request routing-engine login other-routing-engine
re0> show version
re0> exit
```

15. If required, reactivate the NSR and GRES features and save the configuration change to both Routing Engines.

```
re1> edit
re1# activate routing-options nonstop-routing
re1# activate chassis redundancy graceful-switchover
re1# commit synchronize and-quit
```

16. (Optional) We recommend transferring routing control back to the original master Routing Engine after verifying that all replication tasks have been completed.

```
re1> show task replication
re1> request chassis routing-engine master switch
```

17. (Optional) If maintenance mode was enabled before, disable maintenance mode.

```
re0> configure
re0# delete unified-edge gateways ggsn-pgw gateway name service-mode
re0# delete unified-edge gateways sgw gateway name service-mode
re0# commit synchronize
re0# exit
```

Verifying the Upgrade

Ensure that subscribers can access services on the broadband gateway and that traffic can pass. If subscribers were cleared before the upgrade, establish test sessions on all APNs with data transfer.

To verify the upgrade:

1. Perform a functional sanity check when test sessions are active and after they have been cleared.

```
re0> show chassis routing-engine
re0> show chassis fpc detail
re0> show version
re0> show unified-edge ggsn-pgw system interfaces
re0> show unified-edge sgw system interfaces
```

The output of the preceding two commands must show a primary and secondary for both the session and services PIC on the GGSN/P-GW, a primary and secondary

session PIC on the S-GW, and a primary and secondary PFE for each APFE interface. For example:

```
re0> show unified-edge ggsn-pgw system interfaces
```

```
Gateway: GGSN/P-GW Name
```

Interfaces	Members	Operational State	Redundancy Role
ams0	mams-0/0/0	Active	Primary
	mams-10/0/0	Active	Secondary
ams2	mams-0/1/0	Active	Primary
	mams-11/0/0	Active	Secondary
apfe0	pfe-3/0/0	Active	Primary
	pfe-8/0/0	Active	Secondary
apfe1	pfe-3/1/0	Active	Primary
	pfe-8/1/0	Active	Secondary
apfe2	pfe-3/2/0	Active	Primary
	pfe-8/2/0	Active	Secondary

```
re0> show unified-edge sgw system interfaces
```

```
Gateway: S-GW Name
```

Interfaces	Members	Operational State	Redundancy Role
ams1	mams-11/1/0	Active	Primary
	mams-10/1/0	Active	Secondary
apfe3	pfe-3/3/0	Active	Primary
	pfe-8/3/0	Active	Secondary

If any of the configured session PICs (mams interfaces) and PFEs do not appear in this output, contact the next level of support.

Complete the functional sanity check.

```
re0> show unfied-edge ggsn-pgw subscribers
re0> show unfied-edge sgw subscribers
re0> show unified-edge ggsn-pgw status
re0> show unified-edge sgw status
re0> show unified-edge ggsn-pgw statistics
re0> show unified-edge sgw statistics
re0> monitor interface mif.unit
re0> show unified-edge ggsn-pgw charging local-persistent-storage statistics
re0> show unified-edge sgw charging local-persistent-storage statistics
re0> show unified-edge ggsn-pgw charging transfer status detail
re0> show unified-edge sgw charging transfer status detail
re0> show unified-edge ggsn-pgw charging transfer statistics detail
re0> show unified-edge sgw charging transfer statistics detail
re0> show unified-edge ggsn-pgw aaa radius statistics accounting detail
```

2. Repeat the commands described in [“Preparing for the Upgrade” on page 17](#).

Downgrading the Software

To downgrade from Release 12.1W to the previously installed software, follow the upgrade procedure (see [“Upgrading a Router with Redundant Routing Engines to Release 12.1W” on page 19](#)) but replace the software packages with ones corresponding to the appropriate release.



NOTE: You cannot downgrade more than three releases.

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 © 2013, 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. JUNOS 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.