Release Notes: Junos® OS Release 13.2X51-D15 for the EX Series and QFX Series

6 March 2014
Revision 1

Contents

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, EX Series, J Series, M Series, MX Series, PTX Series, QFabric, QFX Series, SRX Series, and T Series.

These release notes accompany Junos OS Release 13.2X51 for the EX Series and QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Junos OS Release Notes for EX Series Switches

These release notes accompany Junos OS Release 13.2X51 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at http://www.juniper.net/techpubs/software/junos/.

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 13.2X51-D15-D15 for the EX Series.

Hardware

- **32-port EX4300 switches**—Two new models of EX4300 switches are now available: EX4300-32F and EX4300-32F-DC. These 32-port 100BASE-X/1000BASE-X switches provide 32 fixed 1-Gigabit Ethernet small form-factor pluggable (SFP) network ports, four built-in 10-Gigabit Ethernet small form-factor pluggable plus (SFP+) uplink ports, and two built-in 40-Gigabit Ethernet quad small form-factor pluggable plus (QSFP+) ports. They support power supply and fan module with front-to-back airflow direction and have a slot for installing an optional uplink module—a 2-port 40-Gigabit Ethernet QSFP+ uplink module that can house two 40-gigabit QSFP+ transceivers or an 8-port 10-Gigabit Ethernet SFP+ uplink module that can house eight 10-gigabit SFP+ transceivers, eight 1-gigabit SFP transceivers, or a combination of eight SFP+ and SFP transceivers. [See EX4300 Hardware Documentation.]

Interfaces

- **Link aggregation group (LAG) bundle hashing configuration**—You can now configure the fields that the LAG hashing algorithm inspects to decide how traffic is placed on the member links in the bundle on an EX4300 switch or EX4300 Virtual Chassis. Configuring the fields used by the LAG hashing algorithm is useful in scenarios where most of the traffic entering the bundle is similar and the traffic needs to be managed within the LAG bundle. [See Configuring the Fields Used by the LAG Hashing Algorithm.]

Related Documentation

- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Known Issues on page 5
- Documentation Updates on page 11
- Migration, Upgrade, and Downgrade Instructions on page 12
- Product Compatibility on page 15

Changes in Behavior and Syntax

There are no changes in default behavior and syntax in Junos OS Release 13.2X51 for EX Series switches.

Related Documentation

- New and Changed Features on page 3
- Known Behavior on page 5
- Known Issues on page 5
- Documentation Updates on page 11
- Migration, Upgrade, and Downgrade Instructions on page 12
- Product Compatibility on page 15

Known Behavior

This section lists the limitations in Junos OS Release 13.2X51-D15 for the EX Series.

High Availability

- On EX4300 Virtual Chassis, the configuration database might get stuck in the Synchronizing state and the Virtual Chassis might not be able to do a switchover after multiple Routing Engine switchovers or mastership changes. As a workaround, issue either the **commit synchronize** command or the **commit synchronize force** command on the master Routing Engine. This is a known software limitation. PR965661

Related Documentation

- New and Changed Features on page 3
- Changes in Behavior and Syntax on page 4
- Known Issues on page 5
- Documentation Updates on page 11
- Migration, Upgrade, and Downgrade Instructions on page 12
- Product Compatibility on page 15

Known Issues

The following issues are outstanding in Junos OS Release 13.2X51-D15. The identifier following the description is the tracking number in our bug database.

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

- Authentication and Access Control
- Bridging and Learning
- Class of Service
- Firewall Filters
- High Availability
- Infrastructure
- Interfaces
- J-Web
- Layer 2 Protocols
- Multicast Protocols
- Network Management and Monitoring
- Port Security
- Routing Protocols
- Virtual Chassis

Authentication and Access Control

- On EX4300 switches, after you clear the MAC addresses from an Ethernet-switching table, the MAC RADIUS authentication sessions is not cleared from the authentication table if the traffic is continuous. PR833888
- On an EX4300 Virtual Chassis, if a large number of clients are authenticated, and then you issue the **clear dot1x interface** command, the system might not remove all entries from the Ethernet switching table. PR867518
- On an EX4300 Virtual Chassis, when a large number of dynamic VLAN users are authenticated on multiple interfaces, dynamic VLAN associations are not removed even after all authenticated 802.1X sessions have cleared. PR881777
- On EX4300 switches, when you enter the **set protocols dot1x authenticator interface all** command, a commit warning might appear.PR892082
- On EX4300 switches, after a client that has been authenticated on a VoIP VLAN interface sends a logoff message, the VoIP VLAN binding on that interface might be deleted. PR896091
- On EX4300 switches, if an access interface is configured in both a data VLAN and a VoIP VLAN, then if IP source guard is enabled on the data VLAN, traffic on the VoIP VLAN might be affected. As a workaround, enable IP source guard on both the data VLAN and the VoIP VLAN. PR898192
- On EX4300 switches, if you change the supplicant mode on an interface, the interface does not fall back to 802.1X authentication from captive-portal authentication. PR920134
- On EX4300 switches, if you restart the firewall process, dynamic filter counters might be created for all authenticated hosts even though only one host has dynamic filter configurations. PR955305
- On EX4300 switches, if you authenticate some MACs through MAC RADIUS in multiple-supplicant mode on an interface, then you disable 802.1X on the interface, then reenable 802.1X on the interface, the MACs on that interface might move to the held state at subsequent authentications. PR957960
- On EX4300 switches, if you authenticate a MAC with the Juniper-Switching-Filter field, the MAC might be put in the held state.PR957995
- On EX4300 switches, in an 802.1X configuration with multiple-supplicant mode, if you clear the Ethernet-switching table, traffic might not be forwarded on a dynamic VLAN. PR959323
- On EX4300 switches, changing the supplicant mode on an 802.1X-enabled interface might clear authenticated sessions on other 802.1X-enabled interfaces. PR969220

Bridging and Learning

- On EX4300 switches and EX4300 Virtual Chassis, after you enable unknown unicast forwarding, the MAC table might not forward packets, and then rebooting the system might cause a Layer 2 address learning daemon (l2ald) core file to be created. PR865485.

Class of Service

- On EX4300 switches, using IEEE 802.1p rewrite rules to set CoS code-point bits in outbound packets might not work properly when both IEEE 802.1p and DSCP rewrite rules are configured on a Layer 3 subinterface. PR914889

Firewall Filters

- On EX4300 switches, the **from interface** ***interface-name*** match condition is not supported on egress firewall filters. PR817979
- On EX4300 switches, policers applied to an egress VLAN-based firewall filter do not work. PR912027
- On EX4300 switches, in an egress port-based firewall filter, the match condition **learn-vlan-id** might not work. PR912191
- On EX4300 switches, in an egress router-based firewall filter, IPv6 Layer 4 headers (**icmp-type**) might not work. PR912483
- On EX4300 switches, filter-based forwarding does not work for routes dynamically inserted through routing protocols. PR913558
- On EX4300 switches, in an egress VLAN-based firewall filter, the IPv4 match condition **interface** might not work. PR918271
- On EX4300 Virtual Chassis, packets that are generated in the CPU and egress out of a non-master FPC port might be subjected to an egress port-based firewall filter and be egress filtered, while packets that egress on a master FPC port might not be egress filtered. PR923659
- On EX4300 switches, the following match conditions configured in IPv6 egress router-based firewall filters and applied to the me0 or vme0 interface do not work: **source-address**, **destination-address**, **source-prefix-list**, and **destination-prefix-list** . PR934196
- On EX4300 switches, the following actions do not work when they are configured in ingress router-based firewall filters for IPv4 or IPv6 and applied to me0 or vme0 interfaces: **port-mirror** and **port-mirror-instance**. PR935140
- On EX4300 switches, the following actions do not work when you configure them in ingress router-based firewall filters for IPv4 or IPv6 and apply them to me0 or vme0 interfaces: **forwarding-class** and **loss-priority**. PR935485
- On EX4300 switches, the ingress router-based firewall filter action **three-color-policer** might not take effect for packets received on me0 and vme interfaces. PR935859

- On EX4300 switches, when a firewall filter is configured with the action **vlan**, traffic is not forwarded to the specified VLAN. PR951798
- On EX4300 Virtual Chassis, if an 802.1X client is authenticated and the server fails, that client might not be re-authenticated, even if the server fail fallback action is configured as **use-cache**, and that client will go into the **Held** state, as shown in the output for the **show dot1x interface** command. PR952144
- On EX4300 switches, if you restart a firewall filter and then reboot the switch, the filter might stop working. PR952306

High Availability

- On EX4300 switches, rebooting the master (FPC1) might cause VRRP to flap. Also, there might be an STP loop for a short period. PR857822
- On EX4300 switches, VRRP on an IRB logical interface stops working if another IRB logical interface's VRRP transitions from backup to master to backup. PR933735

Infrastructure

- When a 40-gigabit link between an EX4300 switch and an EX4550 switch is connected with a DAC cable, the link does not come up if auto-negotiation is set on the EX4300. As a workaround, disable auto-negotiation on the EX4300 switch using the **set interfaces *interface-name* ether-options no-auto-negotiation** command. PR935197
- On EX4300 switches, if you create more than one Ethernet Ring Protection (ERP) instance on the same interface, traffic on that interface might be lost. PR815700
- On EX4300 switches, if you create an Ethernet Ring Protection (ERP) instance with a specified control VLAN, then create a data VLAN for the same ERP instance, traffic might be lost. PR816517
- On EX4300 switches, Ethernet Ring Protection (ERP) fails if the control VLAN is replaced with a different VLAN at runtime. PR817456
- On EX4300 switches, interfaces are not marked as m-router interfaces when they are connected to a multicast router that is not an IGMP querier. PR832877
- On EX4300 switches and EX4300 Virtual Chassis, if you configure more than 512 VSTP instances, the switch might create a core file. PR848278
- On EX4300 switches, proxy ARP is not working after Layer 3 routes are changed. PR889003
- On EX4300 switches, an active interface participating in MVRP might not register and declare the VLANs that are included under **vlan-id-list** in a VLAN range. PR950081
- On EX4300 Virtual Chassis, a VLAN that has already been declared by MVRP might change to being in an idle state after the Virtual Chassis is pre-provisioned and shows as **Idle** in the output of the **show mvrp applicant-state** CLI command. PR950633
- On EX4300 switches, MAC entries might be deleted from the Ethernet-switching table after you change the **interface-mac-limit packet-action** from **drop-and-log** to **drop**. PR951001

- On EX4300 switches, in an RTG, if the member access interfaces are converted to trunk interfaces and are then converted back to access interfaces, the interfaces might lose their association with the VLAN. PR951336
- On EX4300 switches, the jdhcpd process might create a core file if you remove a DHCP server or DHCP relay configuration. PR961684
- On EX4300 switches, when you boot the switch, the **check_configured_tpids: ge-X/X/X: number of configured tpids exceeds the limit(4)** system log message might be displayed. No functionality is affected. PR966061
- On EX4300 switches, the show interfaces interface-name media command shows the speed as 1000 Mbps instead of 100 Mbps for SFP-FX interfaces. PR967119
- On EX4300 switches, Ethernet Ring Protection (ERP) switching time does not happen within 50 ms; ERP data traffic loss occurs for approximately 2 seconds. PR968262
- On EX4300 switches, if you issue the **request system power-off** command, an **Unrecognized command** error message appears. PR968269

Interfaces

- On EX4300 switches, for Layer 3 logical interfaces, the traffic statistics for output packets displayed by the **show interfaces** command are incorrect. PR824894
- On EX4300 switches, setting the inet MTU on a VLAN-tagged aggregated Ethernet interface might cause routing of frames that are larger than the inet MTU. PR910933
- On EX4300 switches, VLAN MAC limit with drop action does not work. PR911753
- On EX4300 switches, when there is a limit on the number of MAC addresses that can be learned on an aggregated Ethernet interface, and the action configured on the interface is to shut down after reaching the MAC limit, the aggregated Ethernet interface might not shut down. PR933168

J-Web

- On EX4300 switches, when you run EZsetup from the J-Web interface, the commit configuration might fail with a timeout error the first time you try to commit the configuration. As a workaround, disconnect the laptop from the switch and then reconnect it, and then use the EZsetup Wizard again. PR858819
- On EX4300 switches, when you commit a configuration using EZSetup, if the laptop becomes disconnected, the J-Web interface reports that the commit operation was successful regardless of whether the commit operation actually succeeded. PR866976
- On EX4300 switches, in the J-Web interface, you cannot change user-defined scheduler map to the default by using **Configure > Class of Service > Assign to Interface, Associate system default scheduler map**. The error message **No change in configuration** appears. As a workaround, use the J-Web CLI editor through **Configure > CLI tools** or use the CLI on the switch. PR954196
- On EX4300 switches, rewrite rules are not populating for physical interfaces in the J-Web interface **Configure > Assign to Interface** page. PR967536

Layer 2 Protocols

- On an EX4300 Virtual Chassis, MAC learning and ARP resolution might fail among interfaces in a VLAN that are connected to the backup when VSTP is enabled on some VLANs and not on others. As a workaround, bring the affected interfaces down and then up again. PR822708
- On EX4300 switches, the MSTI identifier range for MSTP is limited to 1--64. It should be 1–4094.PR846878
- When configuring xSTP on EX4300 switches, you *must add all the interfaces* in the applied VLANs in configurations. For MSTP, configure all interfaces in all VLANs at the **[edit protocols mstp interface]** hierarchy level. PR860226
- EX4300 switches might not switch packets across a VSTP-enabled interface and a redundant trunk group interface that belong to the same VLAN. PR877467
- On EX4300 switches, despite an administrative link being down, child members of an aggregated Ethernet group that is part of a multicast downstream IRB VLAN might be programmed into a multicast route index in the PFE. This situation results in the failure of multicast replication of packets for some VLANs. PR880769

Multicast Protocols

- On an EX4300 switch, when you configure a multicast route, multicast traffic might not go out the egress interface, and the multicast route is not installed in the Packet Forwarding Engine. PR894175
- On EX4300 switches, if MC data packets that fail an RPF check are received on a nonshared tree, the packets might be trapped on the Routing Engine at a high rate, resulting in poor PIM convergence. PR911649
- On EX4300 switches, do not issue the **show igmp snooping membership | match Groups** command if you have a large number (1000+) of groups, because processing uses high CPU. As a workaround, to see a specific group for an interface or all groups for an interface, issue the **show igmp snooping membership** command with filters such as **group** or **interface**. PR914908

Network Management and Monitoring

- On EX4300 switches, there might be a difference of several milliseconds in the results for a two-way delay measurement using an SLA iterator profile and manual on-demand. PR831541
- On EX4300 switches, the **adjacencies** option is not available in the **show ethernet oam connectivity-fault-management** command. PR848776
- On EX4300 switches, two-way Ethernet frame delay measurement (OAM CFM) does not work in centralized mode.PR960168

Port Security

- On EX4300 switches, when you enable MACSec dynamically on a Layer 3 physical interface, the STP state of the port in hardware is set incorrectly to “blocking” and traffic is dropped. As a workaround, delete the family inet/inet6 configuration on the port and reconfigure it. PR912123

Routing Protocols

- On EX4300 Virtual Chassis, issuing the **clear bgp neighbor** command might create a pfex process core file on both master and backup. The BGPV6 session does not come up after the core files are created. PR963855

Virtual Chassis

- On an EX4300 Virtual Chassis, the device control process (dcd) creates core files when mastership is switched over to another Routing Engine. PR818726
- On EX4300 Virtual Chassis, if you issue the **show virtual-chassis vc-port statistics extensive** command, you might see **Undersized packets** and **Runts** error counts incrementing slowly on 40-gigabit Virtual Chassis ports (VCPs). PR952196 closed-not fixed
- On EX4300 Virtual Chassis, if you change the topology from a ring topology to a linear topology and then reboot the Virtual Chassis, one of the members might fail to join the Virtual Chassis. PR953677
- On EX4300 Virtual Chassis, if you renumber the members, a pfex process core file might be created.PR954351
- On EX4300 Virtual Chassis, after a reboot, 10-gigabit Virtual Chassis ports (VCPs) might be shown as **Absent** in **show virtual-chassis vc-port** command output. PR959732
- On EX4300 Virtual Chassis, when line-rate Layer 2 multicast traffic is sent on 10-gigabit uplink modules, a Virtual Chassis split might occur. PR969005

Related Documentation

- New and Changed Features on page 3
- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Documentation Updates on page 11
- Migration, Upgrade, and Downgrade Instructions on page 12
- Product Compatibility on page 15

Documentation Updates

There are no errata or changes in Junos OS Release 13.2X51-D15 documentation.

Related Documentation

- New and Changed Features on page 3

Migration, Upgrade, and Downgrade Instructions

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for the EX Series. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 10.0, 10.4, and 11.4 are EEOL releases. You can upgrade from Junos OS Release 10.0 to Release 10.4 or even from Junos OS Release 10.0 to Release 11.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind. For example, you cannot directly upgrade from Junos OS Release 10.3 (a non-EEOL release) to Junos OS Release 11.4 or directly downgrade from Junos OS Release 11.4 to Junos OS Release 10.3.

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see http://www.juniper.net/support/eol/junos.html .

For information on software installation and upgrade, see the Installation and Upgrade Guide.

Upgrading to Junos OS Release 12.1R2 or Later with Existing VSTP Configurations

If you are upgrading to Junos OS Release 12.1R2 or later from Release 12.1R1 or earlier, ensure that any VSTP configurations on the switch meet the following guidelines. If the VSTP configurations do not meet these guidelines and you run the upgrade, the upgrade fails, and you have to connect the console, change the invalid VSTP configurations, and commit the changed configurations through the console. Guidelines for VSTP configurations are:

- If you have specified physical interfaces for VSTP-configured VLANs, ensure that those interfaces are members of the VLANs specified in the VSTP configuration. If the VSTP configuration specifies **vlan all**, then the interfaces configured at the **[edit protocols vstp vlan all]** hierarchy level must be members of all VLANs.
- If the interfaces are not members of the VLANs in the VSTP configurations but are already added to the VSTP configurations, remove them from those configurations, add them to the VLANs, and then add them back to the VSTP configurations.

This issue is being tracked by PR/736488 in our bug database.

Upgrading from Junos OS Release 10.4R3 or Later

This section contains the procedure for upgrading from Junos OS Release 10.4R3 or later to Junos OS Release 12.2 or later. You can use this procedure to upgrade Junos OS on a standalone EX Series switch with a single Routing Engine and to upgrade all members of a Virtual Chassis or a single member of a Virtual Chassis.

To upgrade Junos OS on an EX6200 or EX8200 switch with dual Routing Engines, see Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure).

To upgrade Junos OS on a switch with a single Routing Engine or on a Virtual Chassis:

1. Download the software package as described in Downloading Software Packages from Juniper Networks.
2. (Optional) Back up the current software configuration to a second storage option. See the *Junos OS Installation and Upgrade Guide* for instructions.
3. (Optional) Copy the software package to the switch. We recommend that you use FTP to copy the file to the **/var/tmp** directory.

   This step is optional because you can also upgrade Junos OS using a software image that is stored at a remote location.
4. Install the new software package on the switch:

   ```
   user@switch> request system software add package
   ```

   Replace ***package*** with one of the following paths:

   - **/var/tmp/*package*.tgz**—For a software package in a local directory on the switch
   - **ftp://*hostname/pathname/package*.tgz** or **http://*hostname/pathname/package*.tgz**—For a software package on a remote server

package.tgz is the name of the package; for example, **jinstall-ex-4200-11.4R1.8-domestic-signed.tgz**.

To install software packages on all switches in a mixed EX4200 and EX4500 Virtual Chassis, use the **set** option to specify both the EX4200 package and the EX4500 package:

```
user@switch> request system software add set [package package]
```

To install the software package on only one member of a Virtual Chassis, include the **member** option:

```
user@switch> request system software add package member member-id
```

Other members of the Virtual Chassis are not affected. To install the software on all members of the Virtual Chassis, do not include the **member** option.

NOTE: To abort the installation, do not reboot your device. Instead, finish the installation and then issue the **request system software delete** *package*.tgz command, where *package*.tgz is the name of the package; for example, **jinstall-ex-8200-11.4R1.8-domestic-signed.tgz**. This is the last chance to stop the installation.

5. Reboot the switch to start the new software:

   ```
   user@switch> request system reboot
   ```

   To reboot only a single member in a Virtual Chassis, include the **member** option:

   ```
   user@switch> request system reboot member
   ```

6. After the reboot has finished, log in and verify that the new version of the software is properly installed:

   ```
   user@switch> show version
   ```

7. Once you have verified that the new Junos OS version is working properly, copy the version to the alternate slice to ensure that if the system automatically boots from the backup partition, it uses the same Junos OS version:

   ```
   user@switch> request system snapshot slice alternate
   ```

   To update the alternate root partitions on all members of a Virtual Chassis, include the **all-members** option:

   ```
   user@switch> request system snapshot slice alternate all-members
   ```

Upgrading to a Controlled Version of Junos OS

Starting in Junos OS Release 13.2X50-D15, two versions of a Junos OS image—a controlled version that supports Media Access Control Security (MACsec) and a domestic version that does not support MACsec—are available for EX Series switches. In previous Junos OS releases for EX Series switches, the domestic version of Junos OS was the only available Junos OS. If you want to enable Media Access Control Security (MACsec), you must install the controlled version of Junos OS in your switch.

If you are upgrading your switch between the domestic version of Junos OS and the controlled version of Junos OS, keep the following issues in mind:

- You can use NSSU to upgrade or downgrade from a domestic version of Junos OS to a controlled version of Junos OS. You cannot use NSSU to upgrade or downgrade from a controlled version of Junos OS to a domestic version of Junos OS, however.
- In a Virtual Chassis, all member switches must be running the same release of Junos OS. If you connect member switches that are running domestic and controlled versions of the same Junos OS release, the switches do successfully join together in a Virtual Chassis. To support MACsec, however, all member switches in the Virtual Chassis must be running the *controlled* version of Junos OS.

The upgrade or downgrade procedure from a domestic version of Junos OS to a controlled version of Junos OS is, otherwise, identical to any other Junos OS upgrade. See Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure) or Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure).

Related Documentation

- New and Changed Features on page 3
- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Known Issues on page 5
- Documentation Updates on page 11
- Product Compatibility on page 15

Product Compatibility

- Hardware Compatibility on page 15

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guide for the product.

To determine the features supported on EX Series switches in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at: http://pathfinder.juniper.net/feature-explorer/

Related Documentation

- New and Changed Features on page 3
- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Known Issues on page 5
- Documentation Updates on page 11
- Migration, Upgrade, and Downgrade Instructions on page 12

Junos OS Release Notes for the QFX Series

These release notes accompany Junos OS Release 13.2X51 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at http://www.juniper.net/techpubs/software/junos/.

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 13.2X51-D15 for the QFX Series. To view the entire set of software information in PDF format, see the Complete Software Guide for Junos OS for the QFX Series.

Hardware

QFX5100-96S—The Juniper Networks QFX5100 line of switches is the next generation of data center fixed-configuration access and aggregation switches. The QFX5100-96S model is a 10-Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) high density access switch or fixed configuration aggregation switch. The QFX5100-96S has 96 SFP+ ports and 8 Quad SFP+ (QSFP+) ports. Each SFP+ port can operate as a native 10-Gbps port or as a 1-Gbps port. QSFP+ ports 96 and 100 can operate at native 40-Gbps speed or as 4 independent 10-Gbps port speeds. When you channelize the interfaces on ports 96 and 100, ports 97, 98, 99, 101, 102 and 103 are disabled. The 8 QSFP+ ports can be used as either access ports or as uplinks. The QFX5100-96S has a 2 U form factor and comes standard with redundant fans and redundant power supplies. The model can

be ordered with either ports-to-FRUs or FRUs-to-ports airflow and with AC or DC power supplies. [See QFX5100 Switch Hardware Overview.]

Interfaces and Chassis

- **Auto-channelization support (QFX5100 Switches)**—Enables the 40-Gbps QSFP+ ports to be channelized by default if any of the four channels on a 40-Gbps QSFP+ port receive data, unless you have already configured channelization at the chassis level or at the port level. Auto-channelization is not supported on interfaces contained in expansion modules or on Virtual Chassis ports. You can disable auto-channelization by including the **disable-auto-speed-detection** statement at the **[edit chassis fpc** *slot-number* **pic** *pic-number* **(port** *port-number* **| port-range** *port-range-low port-range-high***) channel-speed]** hierarchy level. Auto-channelization is not supported on the QFX5100-96S. [See Channelizing Interfaces on QFX3500, QFX3600, and QFX5100 Switches.]

Layer 3 Features

- **Enhanced filter classification of CPU generated packets (QFX5100 switch)**—Enables you to apply egress firewall filters to a loopback interface so that you can set the forwarding class and DSCP bit value for packets that originate on the switch itself. This feature gives you very fine control over the classification of CPU generated packets. For example, you might want to assign different DSCP values and forwarding classes to traffic generated by different routing protocols so that the traffic for those protocols can be treated in a differentiated manner by other devices. [See Overview of Firewall Filters.]

Multiprotocol Label Switching (MPLS)

- **MPLS statistics (QFX5100 switch)**—Enables you to configure Multiprotocol Label Switching (MPLS) so that it periodically gathers traffic statistics about all MPLS sessions, including transit sessions. This is a powerful tool for monitoring and debugging label-switched paths. [See Configuring MPLS to Gather Statistics.]
- **MPLS automatic bandwidth allocation (QFX5100 switch)**—Enables you to configure MPLS so that tunnels automatically adjust their bandwidth allocation based on the volume of traffic flowing through them, which saves you the work of monitoring tunnels and reprovisioning them based on usage. You can configure an LSP with minimal or no bandwidth, and rely on this feature to dynamically adjust the bandwidth allocation based on current traffic patterns. The bandwidth adjustments do not interrupt traffic flow through the tunnel. [See Configuring Automatic Bandwidth Allocation for LSPs.]
- **Policer action for MPLS firewall filter (QFX5100 switch)**—Enables you to configure an MPLS firewall filter with a policer action. This gives you the ability to limit traffic flow per LSP or per class. [See Firewall Filter Match Conditions and Actions.]

Network Management and Monitoring

- **Automation enhancements (QFX5100 switches)**—The QFX5100 switch automation enhancements introduced in Junos OS Release 13.2X51-D15 are designed to support the increasing needs of large data centers for more automation and programmability.

These enhancements are available in a separate download of Junos OS. You can now run unsigned programs, such as programs that you develop with Python, Chef, and Puppet. [See Automation Enhancements for QFX5100 Overview.]

- **Network analytics feature enhancements (QFX5100 switches)**—The network analytics feature provides visibility into the performance and behavior of the data center infrastructure by enabling traffic and queue monitoring. Network analytics enhancements add support for the configuration of collectors, resource types, resource profiles, export profiles, and the Google Protocol Buffer (GPB) streaming data format. Feature enhancements also include changes to CLI statements and hierarchies. After you upgrade to Junos OS Release 13.2X51-D15, any network analytics configurations you used in previous releases will be deprecated, and you must reconfigure this feature using the new CLI statements. You configure network analytics at the [**edit services analytics**] hierarchy level. [See Network Analytics Overview.]

Routing Protocols

- **Support for 64 way ECMP (QFX5100 switch)**—-Enables a Juniper Networks QFX5100 switch to install as many as 64 parallel routes in a routing table and load-balance across all 64 paths. This feature allows you to install the switch as a leaf in a CLOS architecture and connect to as many as 64 spines. This capability is for BGP/ISIS/OSPF, not for MPLS protocols. [See Configuring ECMP Next Hops for RSVP and LDP LSPs for Load Balancing .]
- **Expanded support for advertising multiple paths to a destination in BGP (QFX5100 switch)**—Now supports graceful restart and additional address families. Previously, graceful restart was not supported and only the IPv4 address family was supported with the BGP add-path feature. Now the following address families are supported:
  - IPv4 unicast (net unicast)
  - IPv6 unicast (inet6 unicast)
  - IPv4 labeled unicast (inet labeled-unicast)
  - IPv6 labeled unicast (inet6 labeled-unicast)

  [See Example: Advertising Multiple BGP Paths to a Destination.]
- **Support for BMP Version 3 (QFX5100 switch)**-QFX switches support the BGP monitoring protocol (BMP) version 3. BMP allows a remote device (the BMP station) to monitor BGP as it is running on a routing device or group of routing devices. [See Configuring BGP Monitoring Protocol Version 3.]

Software Upgrade

- **In-Service Software Upgrade (QFX5100 switch)** An in-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with minimal disruption on the control plane and with minimal disruption of traffic. During an ISSU, the Junos OS runs in two separate virtual machines (VMs)—one VM is in the master role acting as the master Routing Engine, and the other VM is in the backup role acting as the backup Routing Engine. The Junos OS is upgraded on the backup VM. After a successful software upgrade, the backup VM then becomes the master VM, and the original master VM is no longer needed and is shut down.

  [See Understanding In-Service Software Upgrade.]

System Management

- **Zero Touch Provisioning (QFX5100 switch)**—Zero Touch Provisioning allows you to provision new Juniper Networks switches in your network automatically without manual intervention. When you physically connect a switch to the network and boot it with a default configuration, it attempts to upgrade the Junos OS software automatically and autoinstall a configuration file from the network.

  The switch uses information that you configure on a Dynamic Host Configuration Protocol (DHCP) server to locate the necessary software image and configuration files on the network. If you do not configure the DHCP server to provide this information, the switch boots with the preinstalled software and default configuration.

  The Zero Touch Provisioning process either upgrades or downgrades the Junos OS version. [See Understanding Zero Touch Provisioning.]

Related Documentation

- Changes in Behavior and Syntax on page 19
- Known Behavior on page 20
- Known Issues on page 21
- Resolved Issues on page 24
- Documentation Updates on page 25
- Migration, Upgrade, and Downgrade Instructions on page 26
- Product Compatibility on page 28

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 13.2X51 for the QFX Series.

- MC-LAG
- Network Management

MC-LAG

- On a QFX5100 switch, configuration of the **minimum-interval milliseconds**statement for liveness detection on a Multichassis Link Aggregation Group (MC-LAG) must be 1000 milliseconds or greater. Subsecond timers are not supported in Junos OS Release 13.2X51-D10 and later. If a timer, lower than 1000 milliseconds timer is configured, it will impact the MC-LAG state.

Network Management

- The network analytics feature enhancements include important changes to the CLI statements and hierarchies. After you upgrade to Junos OS Release 13.2X51-D15, network analytics configurations you used in previous releases will be deprecated, and you must reconfigure this feature using the new CLI statements. For more information, see the Summary of CLI Changes.

Related Documentation

- New and Changed Features on page 16
- Known Behavior on page 20
- Known Issues on page 21
- Resolved Issues on page 24
- Documentation Updates on page 25
- Migration, Upgrade, and Downgrade Instructions on page 26
- Product Compatibility on page 28

Known Behavior

This section lists the limitations in Junos OS Releases 13.2X51 for the QFX Series.

Network Management and Monitoring

- If a QFX5100 switch drops traffic because of an ingress firewall filter, the switch does not generate an sFlow technology monitoring flow sample packet that contains this dropped traffic.
- On the QFX5100 switch, the J-Web interface is not supported. As a result, the **web-management** configuration statement in the **[edit system services]** hierarchy level is not available in the CLI.
- Although the Chef for Junos OS client is bundled with the automation enhancements for QFX5100 switches, the Chef netdev cookbook does not yet support Chef for Junos OS.

Traffic Management

- On a QFX5100 switch, CPU-generated host outbound traffic is forwarded on the network-control forwarding class, which is mapped to queue 7. If you use the default scheduler, the network-control queue receives a guaranteed minimum bandwidth

(transmit rate) of 5 percent of port bandwidth. The guaranteed minimum bandwidth is more than sufficient to ensure lossless transport of host outbound traffic.

However, if you configure a scheduler, you must ensure that the network-control forwarding class (or whatever forwarding class you configure for host outbound traffic) receives sufficient guaranteed bandwidth to prevent packet loss.

If you configure a scheduler, we recommend that you configure the network-control queue (or the queue you configure for host outbound traffic if it is not the network-control queue) as a strict-high priority queue. Strict-high priority queues receive the bandwidth required to transmit their entire queues before other queues are served.

NOTE: **As with all strict-high priority traffic, if you configure the network-control queue (or any other queue) as a strict-high priority queue, you must also create a separate forwarding class set (priority group) that contains only strict-high priority traffic, and apply the strict-high priority forwarding class set and its traffic control profile (hierarchical scheduler) to the relevant interfaces.**

- You cannot apply classifiers and rewrite rules to IRB interfaces because the members of an IRB are VLANs, not interfaces. You can apply classifiers and rewrite rules to Layer 2 logical interfaces and Layer 3 physical interfaces that are members of VLANs that belong to IRB interfaces.

Related Documentation

- New and Changed Features on page 16
- Changes in Behavior and Syntax on page 19
- Known Issues on page 21
- Resolved Issues on page 24
- Documentation Updates on page 25
- Migration, Upgrade, and Downgrade Instructions on page 26
- Product Compatibility on page 28

Known Issues

The following issues are outstanding in Junos OS Release 13.2X51-D15. The identifier following the description is the tracking number in our bug database.

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

- **Filters**
- **Interfaces and Chassis**
- **Layer 2 Features**

- Multiprotocol Label Switching (MPLS)
- Network Management
- Routing Protocols
- Services
- System Management

Filters

- On a QFX5100 switch, after upgrading software using ISSU FIP snooping sessions might stop working. To restore FIP snooping for all new sessions, deactivate and then reactivate FIP snooping. PR965727
- After ISSU, if you delete the filters and try to program new filters, you might be restricted to 768 entries. PR966445
- On a QFX5100 switch, when you perform an in-service software upgrade (ISSU), interfaces might go down and up if Link Aggregation Control Protocol (LACP) is configured in fast mode. As a workaround, configure LACP in slow mode, and disable the distributed periodic packet management daemon (ppmd). PR965918
- ISSU cannot be used to upgrade to Junos OS with enhanced automation for QFX5100 switches. If ISSU is used to upgrade a JUNOS OS image with enhanced automation for QFX5100, any Chef and Puppet packages are lost. You will need to manually install both Puppet and Chef libraries. PR966947
- ISSU cannot be used to upgrade Junos OS images that already have enhanced automation for QFX5100 switches installed. You may use ISSU to upgrade from a standard Junos OS image to an image that has Junos OS with enhanced automation for QFX5100 switches.PR966950

Interfaces and Chassis

- On a QFX5100 switch, the multicast PIM dual-DR mode is not supported in Junos OS Release 13.2X51-D10 or later, even though this feature is supported on other QFX Series devices. PR897618
- On a QFX5100 switch, the output of the **show interfaces *gr-fpc/pic/port*** command for a GRE tunnel interface does not display the proper statistics for encapsulated traffic. PR932561
- If you are running **tcpdump** on the console of a QFX5100 switch, it might cause system instability or cause protocols such as STP or LACP to fail. PR932592
- On a QFX5100 switch, you cannot enable the **minimum-links** statement at the **[edit groups]** CLI hierarchy level. As a workaround, enable the **minimum-links** statement at the **[edit interfaces]** CLI hierarchy level. PR932622
- On a QFX5100 switch, if you apply a firewall filter to the loopback interface, the filter might not discard BFD packets headed to the CPU as expected. PR937408
- On a QFX5100 switch, you cannot configure multichassis link aggregation when Multiple Spanning Tree Protocol (MSTP) or VLAN Spanning Tree Protocol (VSTP) is enabled. PR939049

- On a QFX5100 switch, if you issue the **show interfaces ae** command, the output for aggregated Ethernet logical interfaces might display incorrect information for input and output rates. PR936220
- If a 40-Gbps to 10-Gbps breakout cable is removed and replaced by a 40-Gbps cable, the port's status LED remains unchanged when auto-channelization is enabled. The status LED is lit solid green. PR967471

Layer 2 Features

- On a QFX5100 switch, when the system mode is in default-mode, the latency for 10-Gigabit Ethernet ports in cut-through mode is the same as it is for store-and-forward mode. This issue does not apply to 40-Gigabit Ethernet ports. PR958957

Multiprotocol Label Switching (MPLS)

- On a QFX5100 switch acting as an MPLS penultimate-hop popping (PHP) router, an MPLS label route with a BOS (bottom of the stack) next hop will consume one filter entry and one extra next-hop entry. The total number of filter entries used will be the number of next hops in the system with PHP and BOS operation. PR922969
- On a QFX5100 switch, the system does not collect accurate MPLS statistics if you configure the collection interval to be less than 1 minute or greater than 30 minutes. The default interval is 300 seconds. PR953576 and PR959586

Network Management

- On a QFX5100 switch, the minimum configurable queue statistics polling interval is 10 milliseconds. However, the actual queue statistics polling interval differs from the configured polling interval by approximately 5 milliseconds. PR911015

Routing Protocols

- On a QFX5100 switch, BFD timer values of less than 1 second are not supported. PR942035
- On a QFX5100 switch, when you delete the OSPF configuration from an interface, the OSPF and IS-IS routing protocols transition down and up on all other configured interfaces. PR933536

Services

- If you enable STP on a QFX5100 switch on which you also configure port mirroring, port mirroring works intermittently.PR931633

System Management

- When using an USB drive to install automation enhancements for QFX5100 switches, the Puppet and Chef packages are not bundled with Junos OS. Chef and Puppet packages must be separately installed. PR970371

Related Documentation

- New and Changed Features on page 16
- Changes in Behavior and Syntax on page 19
- Known Behavior on page 20
- Resolved Issues on page 24
- Documentation Updates on page 25
- Migration, Upgrade, and Downgrade Instructions on page 26
- Product Compatibility on page 28

Resolved Issues

This section lists the issues fixed in the Junos OS Release 13.2X51 for the QFX Series.

- Class of Service (CoS)
- Interfaces and Chassis

Class of Service (CoS)

- On a QFX5100 switch, issuing the **show interfaces queue** *interface-name* and **show interfaces statistics** *interface-name* commands does not display the correct traffic rates. PR894390

Interfaces and Chassis

- On a QFX5100 switch, when you enable IGMP snooping on a VLAN, IPv6 multicast traffic is not flooded within the VLAN. PR925141
- On a QFX5100 switch, if you remove the service ID from a multichassis link aggregation group (MC-LAG) configuration, and then add it back to the configuration, single-homed ARP entries might not synchronize properly with MC-LAG peers. PR929720
- On a QFX5100 switch, do not use the unified forwarding table **lpm-profile** for IPv6 traffic. This profile does not work for IPv6 traffic. PR929753
- If you create a virtual routing instance on a QFX5100 switch and configure a routed VLAN interface (RVI) or integrated routing and bridging (IRB) interface under the routing instance, do not configure a multichassis link aggregation group (MC-LAG) interface

to participate in the RVI or IRB. This combination is not supported with virtual routing instances. PR934379

- On a QFX5100 switch, integrated routing and bridging (IRB) MAC address synchronization is not supported, but you can use the Virtual Router Redundancy Protocol (VRRP) instead. As a workaround, configure VRRP on IRB interfaces that host multichassis LAG (MC-LAG) interfaces. PR936512
- On a QFX5100 switch, the **multichassis-lag-replicate-state** statement is not supported at the **[edit vlans]** CLI hierarchy level. As a workaround, enable the **multichassis-lag-replicate-state** statement globally. PR937018
- On a QFX5100 switch, you cannot issue interface range commands for channelized interfaces, As a workaround, use interface commands instead of interface range commands. PR937788
- On a QFX5100 switch, even when traffic is flowing normally, the output of the **show interfaces et-*fpc/pic/port*** and **show interfaces et-*fpc/pic/port:[0-3]*** commands does not display accurate bits per second (bps) information for the **Input rate** field. PR939128
- On a QFX5100 switch, autonegotiation of interfaces is disabled by default for 1-Gigabit Ethernet fiber ports. For these links to be brought online (up), you must disable autonegotiation on the peer interfaces. In addition, If you issue the **show interfaces *interface-name* extensive** command for an SFP access port with a 1-Gigabit optical copper transceiver installed, the output incorrectly shows the media type as **fiber**, if the port parameter is not configured in the **interfaces ge-0/0/*port*** statement in the **[edit]** hierarchy level. As a workaround, remove and reinsert the transceiver. PR939439
- On a QFX5100 switch, configuration of the **minimum-interval *milliseconds*** statement for liveness detection on a multichassis link aggregation group (MC-LAG) must be 1000 milliseconds or greater. Subsecond timers are not supported in Junos OS Release 13.2X51-D10. PR942563

Related Documentation

- New and Changed Features on page 16
- Changes in Behavior and Syntax on page 19
- Known Behavior on page 20
- Known Issues on page 21
- Documentation Updates on page 25
- Migration, Upgrade, and Downgrade Instructions on page 26
- Product Compatibility on page 28

Documentation Updates

This section lists the errata and changes in Junos OS Release 13.2X51 documentation.

Network Management and Monitoring

- The Overview of QFX5100 Switch Automation Enhancements refers the reader to the Chef for Junos OS Getting Started Guide for more information about Chef for Junos OS. However, the Chef for Junos OS documentation is not yet available.

System Management

- The **request app-engine** and **show app-engine** commands are not documented for the QFX5100 switch in Junos OS Release 13.2X51-D10.

Related Documentation

- New and Changed Features on page 16
- Changes in Behavior and Syntax on page 19
- Known Behavior on page 20
- Known Issues on page 21
- Resolved Issues on page 24
- Migration, Upgrade, and Downgrade Instructions on page 26
- Product Compatibility on page 28

Migration, Upgrade, and Downgrade Instructions

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

- Upgrading Software on QFX5100 Standalone Switches on page 26

Upgrading Software on QFX5100 Standalone Switches

When upgrading or downgrading Junos OS, always use the jinstall package. Use other packages (such as the jbundle package) only when so instructed by a Juniper Networks support representative. For information about the contents of the jinstall package and details of the installation process, see the Junos OS Installation and Upgrade Guide and Junos OS Basics in the QFX Series documentation.

The download and installation process for Junos OS Release 13.2 is the same as for previous Junos OS releases.

If you are not familiar with the download and installation process, follow these steps:

1. In a browser, go to http://www.juniper.net/support/downloads/junos.html .

   The Junos Platforms Download Software page appears.

2. In the QFX Series section of the Junos Platforms Download Software page, select the QFX Series platform for which you want to download the software.

3. Select **13.2** in the Release pull-down list to the right of the Software tab on the Download Software page.

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 13.2 release.

   An Alert box appears.

5. In the Alert box, click the link to the PSN document for details about the software, and click the link to download it.

   A login screen appears.

6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Download the software to a local host.
8. Copy the software to the device or to your internal software distribution site.
9. Install the new jinstall package on the device.

   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.

   Customers in the United States and Canada use the following command:

   ```
   user@host> request system software add
   source/jinstall-qfx-5-13.2X51-D15.3-domestic-signed.tgz reboot
   ```

   Replace ***source*** with one of the following values:

   - ***/pathname***—For a software package that is installed from a local directory on the switch.
   - For software packages that are downloaded and installed from a remote location:
     - **ftp://*hostname/pathname***
     - **http://*hostname/pathname***
     - **scp://*hostname/pathname*** (available only for Canada and U.S. version)

   Adding the **reboot** command reboots the switch after the upgrade is installed. When the reboot is complete, the switch displays the login prompt. The loading process can take 5 to 10 minutes.

   Rebooting occurs only if the upgrade is successful.

   NOTE: After you install a Junos OS Release 13.2 jinstall package, you can issue the request system software rollback command to return to the previously installed software.

Related Documentation

- New and Changed Features on page 16
- Changes in Behavior and Syntax on page 19

Product Compatibility

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guide for the product.

To determine the features supported on QFX Series switches in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at: http://pathfinder.juniper.net/feature-explorer/

Related Documentation

Third-Party Components

This product includes third-party components. To obtain a complete list of third-party components, see Copyright and Trademark Information.

For a list of open source attributes for this Junos OS release, see Open Source: Source Files and Attributions.

Finding More Information

For the latest, most complete information about known and resolved issues with Junos OS, see the Juniper Networks Problem Report Search application at: http://prsearch.juniper.net .

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and

hardware platform for your network. Find Feature Explorer at: http://pathfinder.juniper.net/feature-explorer/.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at: http://www.juniper.net/techpubs/content-applications/content-explorer/.

Documentation Feedback

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

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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales 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/customers/support/downloads/710059.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: http://kb.juniper.net/InfoCenter/
- 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 located at 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, visit us at http://www.juniper.net/support/requesting-support.html .

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

`user@host>` **request support information** | **save** *filename*

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net/pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to **support@juniper.net**. For documentation issues, fill out the bug report form located at https://www.juniper.net/cgi-bin/docbugreport/.

Revision History

6 March 2014—Revision 1, Junos OS for the EX Series and QFX Series, Release 13.2X51-D15