Release Notes

Published
2025-10-30

Junos OS Release 23.2R2®

Introduction

Junos OS runs on the following Juniper Network's ® products: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series, vMX, vRR, and vSRX. These release notes accompany Junos OS Release 23.2R2. They describe new and updated features, limitations, open and resolved problems in the hardware and software.

You can find release notes for all Junos OS releases at https://www.juniper.net/documentation/product/us/en/junos-os#cat=release_notes.

Table of Contents

Junos OS Release Notes for ACX Series

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for ACX Series routers.

To view features supported on the ACX platforms, view the Feature Explorer using the following links. To see which features are supported in Junos OS Release 23.2R2, click the Group by Release link. You can collapse and expand the list as needed.

- ACX710
- ACX5448-D
- ACX5448-M
- ACX5448

What's Changed

IN THIS SECTION

Learn about what changed in this release for ACX Series routers.

EVPN

- **Limit on number of IP address associations per MAC address per bridge domain in EVPN MAC-IP database**--By default, devices can associate a maximum of 200 IP addresses with a single MAC address per bridge domain. We provide a new CLI statement to customize this limit, `mac-ip-limit` statement at the `[edit protocols evpn]` hierarchy level. In most use cases, you don't need to change the default limit. If you want to change the default limit, we recommend that you don?t set this limit to more than 300 IP addresses per MAC address per bridge domain. Otherwise, you might see very high CPU usage on the device, which can degrade system performance.

  [See mac-ip-limit.]

Interfaces and Chassis

- Starting in Junos OS release 23.2R1 and Junos OS Evolved release 23.2R1-EVO, the output of `show chassis power` command displays the state of the power supply in PTX10003 and QFX10003 platforms

  [See show chassis power.]

- When all the members of the AE have the same speed (x) and no mixed speed configured. If you change the speed value of any member of the AE to a value other than x, the commit succeeded in earlier releases. From this release, the commit fails. When there are et interfaces with different speeds and you want them to be part of an AE interface. If you change the speed of all the members of the interfaces to be the same speed (x), configure the AE interface, and commit, the commit failed in earlier releases. From this release, such commits succeed.

General Routing

- Before this change most list were ordered by the sequence in which the user configured the list items, for example a series of static routes. After this change the list order is determined by the system with items displayed in numerical sequence rather than by the order in which the items were configured. There is no functional impact to this change.

- ACX7509. NOTE: In the CLI using the command request chassis feb slot slot-number offline if you make the primary FEB offline, a traffic loss warning message is displayed and the FEB offline request is rejected. If offline/restart is still intended for primary FEB, use force option in addition to the command. WARNING message displayed in the CLI: "warning: RCB and FEB work in the paired slot mode. FEB %s offline/restart will result in traffic loss and does not cause a switchover. Please re-try after initiating a mastership switchover using 'request chassis routing-engine master switch' CLI. If offline/restart is still intended, use 'force' option in addition to this CLI."

- **`ephemeral-db-support` statement required to configure MSTP, RSTP, and VSTP in the ephemeral configuration database (ACX Series, EX Series, and QFX Series)**--To configure Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), or VLAN Spanning Tree Protocol (VSTP) in the ephemeral configuration database, you must first configure the `ephemeral-db-support` statement at the `[edit protocols layer2-control]` hierarchy level in the static configuration database.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

Junos XML API and Scripting

- **Ability to commit extension-service file configuration when application file is unavailable**—When you set the `optional` option at the **edit system extension extension-service application file *file-name*** hierarchy level, the operating system can commit the configuration even if the file is not available at the **/var/db/scripts/jet** file path.

  https://www.juniper.net/documentation/us/en/software/junos/jet-developer/topics/ref/statement/file-edit-system-jet.html

Network Management and Monitoring

- **NETCONF `<copy-config>` operations support a `file://` URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The NETCONF `<copy-config>` operation supports using a `file://` URI when `<url>` is the target and specifies the absolute path of a local file.

  [See <copy-config>.]

- **`ephemeral-db-support` statement required to configure MSTP, RSTP, and VSTP in the ephemeral configuration database (ACX Series, EX Series, and QFX Series)**—To configure Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), or VLAN Spanning Tree Protocol (VSTP) in the ephemeral configuration database, you must first configure the `ephemeral-db-support` statement at the `[edit protocols layer2-control]` hierarchy level in the static configuration database.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

Routing Protocols

- **Optimized mesh group routes (QFX5110, QFX5120, QFX5130, QFX5700 and ACX Series)**— `show route snooping` for inet.1/inet6.1 table and `show route snooping table inet.1/inet6.1` will display only CE mesh group routes for platforms that support EVPN-MPLS or EVPN-VxLAN multicast. In earlier releases, other mesh groups like the VE mesh group were also displayed.

VPN

- Increase in revert-delay timer range—The `revert-delay` timer range is increased to 600 seconds from 20 seconds.

  [See min-rate.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for ACX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. https://kb.juniper.net/TSB18251 PR1568757
- servo didn't loose lock for 2000 ns asymmetry value now. But i see Servo lost lock if i apply 10000 ns of asymmetry value. This is expected behaviour from the microsemi as If phase offset is >= 1.5us, servo will come out of Phase Lock. So, when you added 3000/4000ns asymmetry, algorhtm would calculate phase offset 1.5us/2us. As a result, servo will lose Phase Lock. PR1764594
- When asymmetry provided has more than 2000 nsec, there is extra overshot which is expected as per Microsemi stack version v4.10.0P3. this is immediately corrected again after few seconds as expected. PR1770123

Open Issues

IN THIS SECTION

Learn about open issues in this release for ACX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- In VPLS MH cases, the standby UNI ifl in backup router will be programmed in disable state, by adding the UNI interface to invalid vpn id in HW. During switch over the UNI ifl will be deleted and will be added under the VPLS instance VPN id. In issue case, UNI interface added under invalid VPN id in backup router is tried to deleted by passing the VPLS instance vpn id, causing the issue. This issue is applicable only for ACX5k series. PR1665178

- When there are more than 1 dhcp server connected to the device and zeroize in initiated then multiple route are added and the file server is not reachable after the zeroize if it is not reachable through the default route.PR1675011
- Reserved buffers may be shown as 0. But internally reserved buffers do get used to queue and transmit traffic on the queue.PR1689183
- The AE stats may show 0 bps for Output traffic. It is a CLI output display issue. It will be fixed in the future releases. It does not impact the traffic output.PR1689185
- FIPS mode is not supported in this release for SRXSME devices.PR1697999
- On ACX5048 and ACX5096 acting as PE (Provider End) routers, when the VPLS (Virtual Private LAN Service) gets switched multiple times between the primary path and backup path after some time programming fails and the software starts throwing errors. It will impact VPLS services.PR1720141
- Release note neededPR1735425
- On ACX1K/2K platforms, when a lo0.x filter is configured under a vrf type routing-instance, any IPv4 transit traffic that makes ARP request to generate to the CE-facing interfaces will fail in ARP resolution due to the ARP request packets are discard by lo0.x filter if no specific term to accept the IPv4 packets PR1737999
- On ACX1K/2K/3K Platforms, MPLS load-balancing on AE (Aggregated Ethernet) interfaces with more than one member link may not work as expected after upgrading Junos to 20.1R1 or later releases. PR1739480
- CoS:ACX5448:On a L3 interface default classifier is ipprec-compatibility, but after reboot another default classifier is taking effect - ieee8021p-default. PR1754547
- Due to software issue with initialization sequence, the PTP encapsulation does not get applied with PTP configuration on ge interfaces. Because of this, PTP feature is impacted on ge interfaces.PR1755852
- Some Junos releases from 21.4R3 to 22.4R3 may show Remote fault state as 'Offline' in show interface by default. PR1764243
- On Junos ACX5448 device with SFP-T optics, speed displays incorrect in CLI when executing `show interface <interface-name>` CLI command will display "Unspecified" speed. Speed value will not be updated properly. There is no traffic impact. PR1764303

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for ACX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- Delegated BFD sessions configured on routing-instance may fail to come up.

  PR1633395

- dc-pfe: HEAP malloc(0) detected! when a VPLS instance is deactivated in ACX5048. PR1692400
- Traffic loss is more than expected with OSPF TI-LFA node- protection enabled and the primary path is down. PR1695292
- Link is not going down physically while disabling the l2circuit configured interface on Junos based ACX5448 platform. PR1703935
- Traffic drops seen after making COS configuration change on ACX710. PR1704589
- L2VPN traffic is dropped as the default MTU is less by 4 bytes. PR1707932
- L3VPN traffic loss and PFE errors can be seen after an LSP Flap. PR1719507
- The Forwarding Engine Board (FEB 0) crashes and impacts traffic when the L2circuit IGP primary path port is down. PR1720827
- [ACX5048] L2circuit might drop forwarding traffic after flaps although it's in UP state; acx_rt_ccc_eth_vpws_vpn_uni_port_add:UNI VPWS port_add failed AC-IFL: <> VPN: <> (-15:Invalid configuration). PR1726711

- A panic reboot will be observed due to deadlock on VMhost platforms. PR1727985
- We may encounter jdhcpd core during initialization. The core in rare, and there is no service impact because of this core (as the process recovers immediately). PR1730717
- Traffic drops on certain ACX platforms after it is upgraded. PR1731081
- EVPN instance traffic will be dropped when hierarchical-scheduler is enabled on the CE interface. PR1732124
- The IPv4 classification and EXP remarking might not work as expected in the IP-MPLS scenario. PR1732509
- After issuing clear vpls mac table command preceded with clear mpls statistics command execution on ACX routers, traffic loss is observed with the failed error message. PR1734600
- The command "show interfaces diagnostics optics" shows Tx laser as enabled even when the port is administratively down. PR1735670
- Crash on all Junos VMhost platforms due to deadlock panic. PR1735843
- Traffic loss in ACX710 and ACX5448 on any-mpls unicast nexthop protocol configuration. PR1742960
- Traffic impact is observed on Junos MX platforms due to the chassisd crash. PR1745442
- The chassis clock status should not move to "holdover" while switching between PTP path alone. PR1745604
- Link remains down after upgrading Junos image or changing the interface speed on Junos based ACX5448 platform. PR1775279
- EVPN type-5 doesn't work properly when route resolution is performed with preserve-nexthop-hierarchy enabled. PR1746964
- QSFP interfaces show additional flap during PFE bringup. PR1747140
- The memory consumption increases due to memory leak. PR1747992
- Interfaces fail to come online post upgrade. PR1750814
- The rewrite rule stops working when classifier is attached to wildcard IFL. PR1753411
- ACX:CoS: Default ieee-8021p classifier not working for UNI interface for L2 services. PR1756150
- Interface flaps leading to PFE crash due to FPC heap corruption. PR1764083
- LACP packets are not forwarded after the reboot. PR1765478

- On ACX710/5448 with hierarchical-scheduler on CE interfaces EVPN ETREE Leaf to LEAF communication is allowed. PR1765486
- For FRR local repair functionality with unilist of unicast next hops(LSP with link protection) does not work when the link is recovered after a failover, there is a mismatch in the unilist next hop entry between Kernel and PFE. PR1770491
- EVO(EVPN Fabric): DHCP packets are getting relayed even after deleting the dhcp relay configuration from the leaf. PR1775275
- RE CPLD firmware version displayed in ACX5448 is corrected. PR1776650
- Junos OS and Junos OS Evolved: Impact of Terrapin SSH Attack (CVE-2023-48795). PR1781732
- TCP window scaling may be not applied to the first TCP packet sent to the client after the three-way handshake, leading to unnecessary segmentation. PR1761242
- SyncE clock get stuck in 'none' or 'abort' state and impact PTP performance. PR1783632

Interfaces and Chassis

- The interface speed gets set to a lower speed when the interface is disabled and enabled because renegotiation of the interfaces happens at the previously negotiated speed. PR1714267

MPLS

- The rpd process crash is observed when RSVP LSP at Juniper transit/ingress router receives RESV message with RESVCONF object in multi vendor deployment. PR1723229

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for ACX Series routers. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

For information about software installation and upgrade, see the https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/software-installation-and-upgrade/software-installation-and-upgrade.html Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 1: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

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

Junos OS Release Notes for cSRX

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for cSRX.

What's Changed

There are no changes in behavior and syntax in this release for cSRX.

Known Limitations

There are no known limitations in hardware or software in this release for cSRX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Open Issues

There are no known issues in hardware or software in this release for cSRX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Resolved Issues

There are no resolved issues in this release for cSRX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Junos OS Release Notes for EX Series

IN THIS SECTION

What's New

Learn about new features introduced in this release for EX Series.

To view features supported on the EX Series platforms, view the Feature Explorer using the following links. To see which features are supported in Junos OS Release 23.2R2, click the Group by Release link. You can collapse and expand the list as needed.

- EX2300
- EX2300-VC
- EX2300 Multigigabit
- EX3400
- EX3400-VC
- EX4100
- EX4100-F
- EX4300 Multigigabit
- EX4400
- EX4400 Multigigabit
- EX4400-24X
- EX4650-48Y
- EX9200

What's Changed

IN THIS SECTION

Learn about what changed in this release for EX Series switches.

EVPN

- **Default behavior changes and new options for the easy EVPN LAG configuration (EZ-LAG) feature**—The easy EVPN LAG configuration feature now uses some new default or derived values, as follows:
  - Peer PE device `peer-id` value can only be 1 or 2.
  - You are required to configure the loopback subnet addresses for each peer PE device using the new `loopback-subnet peer1-subnet` and `loopback peer2-subnet` options at the `[edit services evpn device-attribute]` hierarchy level. The commit script uses these values for each peer PE device's loopback subnet instead of deriving those values on each PE device. The `loopback-subnet` option at the `[edit services evpn device-attribute]` hierarchy level has been deprecated.
  - If you configure the `no-policy-and-routing-options-config` option, you must configure a policy statement called EXPORT-LO0 that the default underlay configuration requires, or configure the new `no-underlay-config` option and include your own underlay configuration.
  - The commit script generates "notice" messages instead of "error" messages for configuration errors so you can better handle `[edit services evpn]` configuration issues.
  - The commit script includes the element names you configure (such as IRB instance names and server names) in description statements in the generated configuration.
- This feature also now includes a few new options so you have more flexibility to customize the generated configuration:
  - `no-underlay-config` at the `[edit services evpn]` hierarchy level—To provide your own underlay peering configuration.
  - `mtu overlay-mtu` and `mtu underlay-mtu` options at the `[edit services evpn global-parameters]` hierarchy level—To change the default assigned MTU size for underlay or overlay packets.

  [See Easy EVPN LAG Configuration.]

General Routing

- Before this change most list were ordered by the sequence in which the user configured the list items, for example a series of static routes. After this change the list order is determined by the system with items displayed in numerical sequence rather than by the order in which the items were configured. There is no functional impact to this change.
- NOTE: In the CLI using the command request chassis feb slot slot-number offline if you make the primary FEB offline, a traffic loss warning message is displayed and the FEB offline request is

rejected. If offline/restart is still intended for primary FEB, use force option in addition to the command. WARNING message displayed in the CLI: "warning: RCB and FEB work in the paired slot mode. FEB %s offline/restart will result in traffic loss and does not cause a switchover. Please re-try after initiating a mastership switchover using 'request chassis routing-engine master switch' CLI. If offline/restart is still intended, use 'force' option in addition to this CLI."

Junos XML API and Scripting

- **Ability to commit `extension-service file` configuration when application file is unavailable**—When you set the `optional` option at the **`edit system extension extension-service application file`** ***`file-name`*** hierarchy level, the operating system can commit the configuration even if the file is not available at the **/var/db/scripts/jet** file path.

  [See file (JET).]

Network Management and Monitoring

- **NETCONF `<copy-config>` operations support a `file://` URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The NETCONF `<copy-config>` operation supports using a `file://` URI when `<url>` is the target and specifies the absolute path of a local file.

  [See <copy-config>.]

- **`ephemeral-db-support` statement required to configure MSTP, RSTP, and VSTP in the ephemeral configuration database (ACX Series, EX Series, and QFX Series)**—To configure Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), or VLAN Spanning Tree Protocol (VSTP) in the ephemeral configuration database, you must first configure the `ephemeral-db-support` statement at the `[edit protocols layer2-control]` hierarchy level in the static configuration database.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

User Interface and Configuration

- **Viewing files with the `file compare files` command requires users to have `maintenance` permission**— The `file compare files` command in Junos OS and Junos OS Evolved requires a user to have a login class with `maintenance` permission.

  [See Login Classes Overview.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for EX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Infrastructure

- When upgrading from Junos OS releases prior to Junos OS Release 21.2 and later, the validation and upgrade might fail. The upgrade requires using the `no-validate` option to complete successfully. PR1568757

Platform and Infrastructures

- On EX4650 devices, one VLAN can be mapped to only on ERPS ring. For example, VLAN 100 can be mapped to only one ERPS ring. This same VLAN 100 cannot be part of another ERPS ring on the same switch. PR1732885
- On EX4400-48F devices, the input-vlan-tagged-frames are not in the expected range while verifying the VLAN Tagged Frames. PR1749391

Virtual Chassis

- The EX4400 device supports multiple uplink modules. Some supports VC port conversion and some doesn't and hence, the recommended procedure is to convert VC port to NW port first and then make sure uplink module is made offline using the `request chassis pic fpc` command before removal. PR1665242

Open Issues

IN THIS SECTION

Learn about open issues in this release for EX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

High Availability (HA) and Resiliency

- Graceful Routing Engine Switchover (GRES) not supporting the configuration of a private route, such as fxp0 , when imported into a non-default instance or logical system. PR1754351

Interfaces and Chassis

- You can configure the routing platform to track IPv6-specific packets and bytes passing through the router. To enable IPv6 accounting, include the route-accounting statement at the [edit forwarding-options family inet6] hierarchy level. By default, IPv6 accounting is disabled. If IPv6 accounting is enabled, it remains enabled after a reboot of the router. To view IPv6 statistics, issue the `show interfaces statistics` operational mode command.

  [See Configuring IPv4 and IPv6 Accounting]. PR717316

Layer 2 Ethernet Services

- If name-server information is changed via CLI after the DHCP subscribers are up, DNS obtained from DHCP server is overwritten by local config. This may result in DNS look up failures in some cases. PR1743611

MPLS

- On Junos QFX5100 and EX4600 platforms in Layer 2 Virtual Private Network (L2VPN) scenarios, when an access port flaps or the port related configuration is deactivated and activated, the traffic ingressing or egressing out of that port gets dropped. PR1775553

Platform and Infrastructure

- On Junos OS EX4300 and EX4300-VC platforms, if zeroize or interface configuration deletion performed, PFEX process crash will se seen when interface/device comes up and there will be traffic loss during the PFE restart. PR1714117
- In a rare scenario, due to timing issues, the Packet Forwarding Engine (PFE) crash is observed on Junos EX4300 platforms. This causes traffic loss until the PFE comes up. PR1720219
- On Junos EX4300-24T/24P when the native CVLAN (Customer Virtual Local Area Network) ID is configured for Q-in-Q setup, the traffic for that particular VLAN gets dropped even if the knob "input-native-vlan-push" is configured. This issue is encountered when the when inner-tag matches 'native-vlan-id' irrespective of the outer tag. PR1722284

- On EX4300 platforms, when the firewall filter applied on the loopback interface is configured with default action as a discard on the DHCP-Relay and a client is connected to a VLAN with DHCP-security and DHCP-Relay enabled, then the DHCP lease renewal unicast packet sent by the DHCP client will be dropped by the loopback filter on the DHCP-Relay. This will eventually lead to service impact. PR1730903
- On EX4300-VC, the Online Insertion and Removal (OIR) of Quad Small Form-factor Pluggable (QSFP) may result in a PFE crash under near-zero idle CPU conditions. PR1733339
- On all EX4300 platforms, traffic is sent on an the aggregated Ethernet interface and sent to the removed child interface from AE (Aggregated Ethernet) where the traffic is lost. PR1749406
- Runt, fragment and jabber counters are not incrementing on EX4300-MPs devices. PR1492605
- On EX2300, EX3400, EX4300-48MP and EX4300 devices, the pause frames counters does not get incremented when pause frames are sent. PR1580560
- When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted may go into a hung state and remain in that state even after the reboot is complete. This may affect traffic after the remote end system comes online and resumes traffic transmission. PR1665800
- On the EX4600 device with SFP-LX10/SFP-SX, after a power cycle/software reboot, all ports are initialized and links are up with auto-negotiation enabled. Few ports are up and traffic flows whereas few ports are up but no traffic flow through them. PR1672583
- On all EX platforms, whenever beacon LED functionality is enabled, there is a mismatch between the physical LED status and the output of the CLI command ?show chassis led? showing incorrect port LED status for interfaces as LED up instead. PR1697678
- On Junos OS platforms, the dcpfe (Dense Concentrator Packet Forwarding Engine) process crash will be observed due to memory fragmentation issue. This is a very rare case and would impact traffic as due to dcpfe failure the PFE restarts, so the interfaces flaps. PR1711860
- On EX4650 and QFX5120-48Y, the SFP-LX interface will not be UP when different Small Form-factor Pluggable(SFP-10GBASE-T and SFP-LX) are plugged in within the same 4 port group. The presence of the 10GE-T SFP resets the speed of the quad back to 10G even if the quad port speed is set to 1G. Normally 10G interface by itself will be up when set to 1G if no other SFP is plugged in. PR1714833
- On EX switches, if 40G DAC(Direct Attach Copper) cables with PN(Part Number) 740-038624 (QSFP+-40G-CU3M) and 740-044512 (QSFP+-40G-CU50CM) are used, links might not come up after software upgrade to Junos 21.4R3-S3 or after a switch reboot (if the switch is running Junos 21.4R3-S3). The switch ports that use these DAC cables are observed to go down after a reboot. PR1752611
- On EX4400 devices, the `set chassis config-button no-clear` command does not work. PR1758042

- On EX2300 VC, the Dot1x authentication flapping in multiple supplicant mode with 100 user scale. PR1767706
- On the peer device ports connected to 24-40 port group from ex4100-48P/T going up for 2-3s during device reboot. PR1775479
- When there are a large number of aggregated (AE) interfaces on a system, deleting all of them together and adding them back can lead to a race condition. This could result in a few of the interfaces not being programmed correctly. PR1781955

Virtual Chassis

- On Junos EX4600 Virtual Chassis (VC), the primary Routing Engine reboots and all-members reboot lead to the PFE Manager hogging logs when SFP-T pluggable is installed in. The PFE Manager hogging logs has no functionality impact.PR1685067
- On EX4600-VC, when the `request system reboot all members` command gets executed, post-reboot one of the VC member/Flexible PIC Concentrator(FPC) might disconnect and join the VC back due to Packet Forwarding Engine (PFE) restart. Traffic loss is seen when FPC is disconnected. PR1700133

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for EX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

EVPN

- After deactivating or activating GBP configuration in the MH AE scenario all tag entries not getting re-learned on leaf nodes in the ethernet-switching table resulting in traffic loss. PR1739878

Interfaces and Chassis

- DCD crash can be seen sometimes while pushing config using API. PR1742124
- Services using the management interface will be affected on all Junos platforms. PR1757936

J-Web

- A PHP vulnerability in J-Web allows an unauthenticated to control important environment variables. PR1736942

Junos Fusion Satellite Software

- Junos Fusion Satellite device will be stuck in the `SyncWait` state. PR1733558

Layer 2 Ethernet Services

- Auto-image-upgrade knob is not present when EX-VC is zeroized and VC is formed. PR1694952
- DHCP binding is not happening in EVPN VXLAN topology with DHCP stateless relay (forward-only). PR1722082
- DHCPv6 security functionality gets effected as DHCPv6 security bindings are not present. PR1731784

- Address allocation for DHCP client fails if 'force-discover' configuration is enabled on client. PR1742696
- Name-server resolution failure might be seen intermittently after zeroize or loading factory default config resulting in MIST on-boarding failure. PR1747800
- The jdhcpd process hangs on receiving a specific DHCP packet. PR1706709

Platform and Infrastructure

- Unable to onboard the VC members after performing ZTP due to the phone-home process sending a blank in the device serial number field while connecting to the redirect server. PR1687926
- EX4400: pps counter does not show correct values for jubmo frames. PR1700309
- With MAC limit and persistent MAC learning configuration l2ald process will crash when MAC is learned through remote peers. PR1706364
- On EX4400 device, the `show chassis environment power-supply-unit` command displays only master member's details. PR1709483
- Certain EX platforms with option-18 configured may hinder the DHCPv6 process. PR1710360
- The interface remains up and LED is still green when the cable is removed. PR1711695
- The LLDP negotiation response is not sent back to PD when perpetual Power over Ethernet (PoE) is enabled on EX4400. PR1713545
- IGMP/MLD queries may get dropped if received on a port on the backup VC member when IGMP/MLD snooping is enabled. PR1716902
- Alarm "PEM is not supported/powered" might be seen after removing the power cable. PR1718825
- Continuous messages indicating duplicate IP address L2ALM_DUPLICATE_IP_ADDR will be seen in MCLAG and VRRP scenario. PR1719868
- Port will be down when the `no-auto-negotiation` command gets configured on EX4400-48F platform. PR1720074
- EX4400 shows incorrect interface et-0/0/0. PR1720257
- On EX2300MP, error messages are observed during reboot/image upgrade. PR1721433
- Invalid "Power Class" value will be observed. PR1722674

- Traffic loss will be observed with vlan tagging and/or vlan normalisation in a specific design (using a looped cable). PR1724675
- The entPhysicalSoftwareRev MIB object returns Junos OS version value for components which do not run Junos OS. PR1725078
- EX4400: After BIOS upgrade device mode gets changed from HGoE to HiGig mode. PR1725683
- FPC temperature value will be exported incorrectly in Telemetry server. PR1726532
- Memory leak is observed on all Junos platforms during ZTP. PR1726603
- Root user is unable to login using public key authentication after reboot or upgrade PR1726621
- Programming of native-vlan-id on the interface fails and MAC is not learned. PR1727112
- On all Junos and Junos Evolved platforms the l2ald process memory usage is seen to increase over time. PR1727954
- EX4400 VC: During upgrade/reboot , fxpc core may be seen in a very rare race condition. PR1728725
- EX4400: While exporting telemetry data, transceiver data is also streamed when there is no transceiver in device itself. PR1729464
- Packets received on a port that is in `LACP Detached` state gets forwarded. PR1730076
- On EX4400 device, PIC2 details might not be not displayed for the `show snmp mib walk entPhysicalVendorType` command. PR1731146
- Traffic for VLAN-id 2 gets dropped in Ethernet-CCC L2 Circuit on the EX4650 platforms. PR1731291
- EX4400: Some log messages may get flooded in heavily loaded system. PR1731345
- The traffic drop will be observed after changing the VSTP VLAN configuration. PR1731522
- The fxpc process crashes when the next hop information is not properly maintained in the PFE table. PR1731548
- Filter term dropping VRRP traffic when "then log" is configured. PR1732271
- The ppmd proces crashes will be seen in EX-VC scenario. PR1733134
- Error logs are seen with a non-vxlan dot1x enabled port. PR1733365
- On EX2300-VC when VCP interfaces are disabled/enabled then tvp_status_led_set error messages are seen. PR1733636

- EX4300-48MP: Device did not come up with USB image when the `request system reboot usb` command gets issued. PR1734925
- Control plane flap, data drop, unexpected behavior of PFE or device is observed when file storage is impacted in a continuous ksyncd process crash scenario. PR1735685
- Port LEDs are not working as expected when the mode is changed from default to EN. PR1735786
- EX4400 shaping rate not working as expected. PR1736790
- A PHP vulnerability in J-Web allows an unauthenticated attacker to control important environment variables. PR1736937
- On EX4400 devices, the `request system halt/power-off` command does not turn off FAN LED's. PR1737500
- VC on EX3400 platforms will not form with 40GBASE-BXSR optics. PR1737524
- Link down due to FEC mismatch on EX4650, EX4400 and Junos based QFX5K platforms using 25G-LR optics. PR1738077
- The 'input-vlan-map push' operation will not work on double-tagged frames. PR1738384
- [QFX5/EX] Error message like 'BRCM-VIRTUAL,brcm_vxlan_port_discard_set(),13034:Failed to set bcm_port_discard_set to 0 for port (61) err(Invalid unit). PR1738404
- On certain EX platforms when 25G DAC in 4x25G is plugged into PIC port does not come up when used as VC. PR1738535
- DHCP offer is dropped at MX and specific EX platforms when an lt interface is used as the transport. PR1738548
- In EVPN-VXLAN scenario DHCP does not work for clients connected on the dot1x port. PR1739730
- Layer 2 traffic will be dropped on VSTP disabled interface. PR1739975
- EX4400 VC : Both mge and ge interfaces are getting created for all ports during master member-id and role swap with line card. PR1740024
- The interface speed is not updated during reboot on Junos EX platforms. PR1740064
- On EX4400-48F, After phc commit in VC, default storm control config has extra xe port config for 0-11 ports and extra ge port config for 37-48 ports. This has no functionality impact. PR1740579
- On EX4400 with pre existing configuration of 1g for the uplink interfaces, it might not come up after 4x10G module insertion event. PR1741724
- DOT1XD_USR_ATHNTICTD_GST_VLAN is not triggered. PR1741867

- On EX4400, on CLI "load factory-default", config loaded does not have VLAN configuration. PR1742114
- Race condition where FLOOD ROUTE DEL event can cause l2ald crash. PR1742613
- Traffic drop will be observed after extended-vni-list configuration change with EVPN-VXLAN scenario. PR1742763
- ZTP:IPV6: EX4300MP: Baseline config is not applying to the device when loading it using shell script. PR1743222
- The l2ald crashes when there is recursive deletion of IFBD or when BGP neighborship is cleared in EVPN-VXLAN multi-homed configuration. PR1743282
- EX Series: Removal of notice about the availability of new POE firmware and the prompt to upgrade the same. PR1743547
- On EX2300/EX3400, unexpected error message during oam boot. PR1744141
- On EX4100 device, VC formation will not happen automatically after zeroize. PR1744190
- Enhancement of PoE Controller Firmware upgrade procedure. PR1744343
- VLAN traffic received over VTEP is being dropped. PR1746998
- LLDP will not work on HGoE VC mode with 40G VCP connections. PR1747095
- PoE ports stop working after the reboot. PR1747128
- [EX/QFX] Under rare situations, 10GBASE-T SFP might be unable to make the peer end deivce linkdown. PR1747277
- Packet drop will be observed due to ARP resolution failure in EVPN-VXLAN scenario. PR1747878
- Connectivity fails intermittently on 802.1x enabled ports. PR1749312
- Incorrect egress MTU errors when larger than 1500 byte packets are sent on L2 ports. PR1751700
- POE Log "Thread 22 (PoE Periodic) ran for ms without yielding" may be seen. PR1751868
- EX4100 : L2ALD_IFBD_COUNT_EXCEED is not generated when exceeded max number of vmember. PR1752756
- Runt frames generate excessive traffic statistics on EX4100/EX4400 platforms. PR1753576
- Traffic impact will be seen for static VoIP VLAN on access interface if same VLAN configured as data VLAN. PR1754474
- The transceiver fails to get detected after the system reboot. PR1754931

- Ports remain down on backup member switch of VC on certain EX4400 platforms after power outage in a rare scenario. PR1755433
- The dcpfe process crash will be seen when L2PT interfaces are configured with multiple protocols. PR1757329
- Whenever IGMP leave request is initiated by receiver unicast traffic to the host IP on the switch port is non-responsive. PR1757431
- On the EX4400 devices, PSM is not detected in the `show chassis hardware` command until AC feed is connected to it. PR1759351
- The configuration was not applied correctly to set the transmit-rate to the same speed as the interface speed. PR1759821
- The fxpc process might crash and cause traffic loss when adding and deleting irb configuration. PR1760229
- The 'input-vlan-map push' operation will not work on double-tagged frames. PR1761220
- LLDP neighborship will not be formed on all Junos devices. PR1763053
- VPLAG information not installed correctly in hardware results in traffic flooding. PR1763116
- LLDP neighborship is not forming in non-master members. PR1764085
- CPU utilization increases and stays high due to pfex_junos process. PR1640045
- MAC entry not ageout in RTG in EX4600-VC after VCP port reconnect. PR1707878
- TDR fails on EX4100 platform. PR1724086
- On EX4100 devices, the weird system connection gets started by the switch. PR1724720
- Error message 'LBCM-L2,pfe_bcm_stp_set_nostp_port_state(),X:handling for lag with no members[op x ifd aeX vid x]' is seen when changing config related to interface. PR1732217
- Multicast will not work if one or more VLANs are removed from the interface having multicast configured. PR1738355
- The PFE process crashed while removing and applying the firewall filters. PR1750828
- In Q-in-Q push/pop configuration for double tagged protocol traffic it is seen that the third VLAN tag is getting swapped instead of getting pushed onto the stack. PR1752898
- Device crash and control plane traffic gets impacted on Junos platforms. PR1753908
- EX4400 Platforms Virtual Chassis (VC) - HGOE enabled causes system crash when system memory becomes unavailable for cumulative protocol daemons traffic. PR1754344

- The interface stats interrupt might be lost resulting in stats not getting updated. PR1755161
- Interface on the server side activates during switch boot-up process on EX4100 platforms. PR1756750
- Multicast traffic will be dropped when IGMP-snooping with bpdu-block-on-edge gets configured. PR1757160
- The ksyncd and vmcore core will be seen on backup RE when GRES is configured. PR1757692
- Node-locked license gets lost on master VC member post reboot. PR1757835
- SNMP Insertion trap not seen while fan removal and insertion. PR1762096
- Memory leak is observed when dot1x authentication is used. PR1766314
- A warning message is seen while installing a license key with an unknown feature. PR1766515
- An unnecessary traffic load on the peer boxes. PR1767190
- [EX46/QFX5K]MTU Errors are counted when receiving packets up to 4 bytes in MTU. PR1770448
- EX4100/4400 : Error message 'COS default: IEEE 802.1ad defaults not specified' upon commit operation. PR1771111
- VLAN change on one port is affecting forwarding plane traffic on other ports to which no changes were done. PR1771222
- License missing on VC member after reboot. PR1771376
- In EVPN-MPLS/EVPN-VxLAN Multi-Home Active/Active scenario, random packet drops are observed. PR1772733
- TDR link status not consistent in CLI. PR1773103
- The DHCP client will not be able to get the IP address. PR1774202
- The RE goes into amnesiac mode upon license check validation failure. PR1775463
- Core dumps for pfex and dot1x seen due to dot1x authentication. PR1778056
- In Virtual-Chassis mode, the EX4100 switch might not boot up upon triggering a manual reboot. PR1778873

Routing Protocols

- The mcscnoopd process will be stuck in resync state after snooping configuration is deleted and added again immediately. PR1699784
- OSPFv3 using the VIP address on the IRB interface will not form adjacencies between peers. PR1737978
- BFD session for BGP remains down in a specific scenario. PR1738074
- Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute. PR1739919
- Memory leak observed when reconfiguring the flow routes. PR1742147
- BGP multipath route is not correctly applied after changing the IGP metric. PR1754935

User Interface and Configuration

- After the device reboot BGP sessions will be down. PR1726731
- Device boots up even with incompatible configuration. PR1730442

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for EX Series switches. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

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

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 2: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

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

Junos OS Release Notes for JRR Series

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for JRR Series Route Reflectors.

What's Changed

There are no changes in behavior and syntax in this release for JRR Series Route Reflectors.

Known Limitations

There are no known limitations in hardware or software in this release for JRR Series Route Reflectors.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Open Issues

There are no known issues in hardware or software in this release for JRR Series Route Reflectors.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Resolved Issues

There are no resolved issues in this release for JRR Series Route Reflectors.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for the JRR Series Route Reflector. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

For information about software installation and upgrade, see the JRR200 Route Reflector Quick Start and Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.

- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 3: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

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

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for Juniper Secure Connect.

What's Changed

There are no changes in behavior and syntax in this release for Juniper Secure Connect.

Known Limitations

There are no known limitations in hardware or software in this release for Juniper Secure Connect.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Open Issues

There are no known issues in hardware or software in this release for Juniper Secure Connect.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Resolved Issues

There are no resolved issues in this release for Juniper Secure Connect.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Junos OS Release Notes for MX Series

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for the MX Series routers.

To view features supported on the MX Series platforms, view the Feature Explorer using the following links. To see which features are supported in Junos OS Release 23.2R2, click the Group by Release link. You can collapse and expand the list as needed.

- MX150
- MX204
- MX240
- MX304
- MX480

- MX960
- MX2008
- MX2010
- MX2020
- MX10003
- MX10008
- MX10016
- vMX

What's Changed

IN THIS SECTION

Learn about what changed in this release for MX Series routers.

Class of Service (CoS)

- You cannot apply a classifier to a physical interface on MX Series routers. On MX Series routers, you must apply the classifier to a logical interface.

EVPN

- **EVPN-VXLAN tracing configuration**— The `set services trace evpn-vxlan` configuration invokes a built-in commit script to generate tracing configurations for troubleshooting EVPN-VXLAN in multiple modules and hierarchies.

  [See trace (EVPN-VXLAN).]

- **Default behavior changes and new options for the easy EVPN LAG configuration (EZ-LAG) feature**— The easy EVPN LAG configuration feature now uses some new default or derived values, as follows:

  - Peer PE device `peer-id` value can only be 1 or 2.
  - You are required to configure the loopback subnet addresses for each peer PE device using the new `loopback peer1-subnet` and `loopback peer2-subnet` options at the `[edit services evpn device-attribute]` hierarchy level. The commit script uses these values for each peer PE device's loopback subnet instead of deriving those values on each PE device. These replace the `loopback-subnet` option at the `[edit services evpn device-attribute]` hierarchy level, which has been deprecated.
  - If you configure the `no-policy-and-routing-options-config` option, you must configure a policy statement called EXPORT-LO0 that the default underlay configuration requires, or configure the new `no-underlay-config` option and include your own underlay configuration.
  - The commit script generates "notice" messages instead of "error" messages for configuration errors so you can better handle `[edit services evpn]` configuration issues.
  - The commit script includes the element names you configure (such as IRB instance names and server names) in description statements in the generated configuration.

  This feature also now includes a few new options so you have more flexibility to customize the generated configuration:

  - `no-underlay-config` at the `[edit services evpn]` hierarchy level—To provide your own underlay peering configuration.
  - `mtu overlay-mtu` and `mtu underlay-mtu` options at the `[edit services evpn global-parameters]` hierarchy level—To change the default assigned MTU size for underlay or overlay packets.

  [See Easy EVPN LAG Configuration.]

.

- **Limit on number of IP address associations per MAC address per bridge domain in EVPN MAC-IP database**—By default, devices can associate a maximum of 200 IP addresses with a single MAC address per bridge domain. We provide a new CLI statement to customize this limit, `mac-ip-limit` statement at the `[edit protocols evpn]` hierarchy level. In most use cases, you don?t need to change the default limit. If you want to change the default limit, we recommend that you don?t set this limit to more than 300 IP addresses per MAC address per bridge domain. Otherwise, you might see very high CPU usage on the device, which can degrade system performance.

  [See mac-ip-limit.]

General Routing

- The `max-db-size` is an optional configuration command on routers having >=32 GB DRAM, for example, on MX960 platform. To enable subscriber-management, use the command set chassis network-services enhanced-ip and set system services subscriber-management enable. The router reboots and comes-up with subscriber-management enabled without max-db-size (optional) configuration and requires only 1 reboot.

- In older Junos Releases, Data Definition Language (DDL) lists were ordered by the sequence in which the user configured the list items, for example a series of static routes. With this change, the list order is determined by the system with items displayed in numerical sequence rather than by the order in which the items were configured. There is no functional impact to this change.

- While running `request system snapshot recovery` command on all VMHost based Routing Engines, disable or stop reporting any warning message.

- **Introduction of extensive option for IPsec security associations (MX Series, SRX Series and vSRX 3.0)** We've introduced the `extensive` option for the `show security ipsec security-associations` command. Use this option to display IPsec security associations with all the tunnel events. Use the existing `detail` option to display upto ten events in reverse chronological order.

  [See show security ipsec security-associations.]

- **New commit check for MAC-VRF routing instances with the encapsulate-inner-vlan statement configured**— We introduced a new commit check that prevents you from configuring an IRB interface and the `encapsulate-inner-vlan` statement together in a MAC-VRF routing instance. Please correct or remove these configurations prior to upgrading to Junos OS 23.2R2 or newer to avoid a configuration validation failure during the upgrade.

  [See encapsulate-inner-vlan.]

- **MTU and TCP MSS not available on service interfaces (MX Series routers)**—You cannot configure the media MTU or TCP MSS on service interfaces (ms, vms, or ams).

  [See mtu (interfaces).]

- **Change in options and generated configuration for the EZ-LAG configuration IRB subnet-address statement**—With the EZ-LAG `subnet-address inet` or `subnet-address inet6` options at the `[edit services evpn evpn-vxlan irb irb-instance]` hierarchy, you can now specify multiple IRB subnet addresses in a single statement using the list syntax `addr1 addr2 ...` . Also, in the generated configuration for IRB interfaces, the commit script now includes default `router-advertisement` statements at the `[edit protocols]` hierarchy level for that IRB interface.

  [See subnet-address (Easy EVPN LAG Configuration).]

- **Media Access Control Security (MACsec) session remains stable when changing exclude-protocol configuration**—When you change the protocols excluded from MACsec using the exclude-protocol protocol-name option at the `[edit security macsec connectivity-association connectivity-association-name]`, the MACsec session remains stable.

  [See exclude-protocol

- **ChaCha20-Poly1305 algorithm deprecation for SSH cipher option**—The ChaCha20-Poly1305 authenticated encryption algorithm is deprecated for SSH cipher option. Configure aes-128-gcm and aes-256-gcm as the encryption algorithm for SSH Cipher option.

  [See ssh (System Services).] PR1783811

Interfaces and Chassis

- When all the members of the AE have the same speed (x) and no mixed speed configured. If you change the speed value of any member of the AE to a value other than x, the commit succeeded in earlier releases. From this release, the commit fails. When there are et interfaces with different speeds and you want them to be part of an AE interface. If you change the speed of all the members of the interfaces to be the same speed (x), configure the AE interface, and commit, the commit failed in earlier releases. From this release, such commits succeed.PR1745893

Junos XML API and Scripting

- **Ability to commit `extension-service file` configuration when application file is unavailable**—When you set the `optional` option at the `[edit system extension extension-service application file file-name]` hierarchy

level, the operating system can commit the configuration even if the file is not available at the **/var/db/scripts/jet** file path.

[See file (JET).]

Network Management and Monitoring

- **NETCONF <copy-config> operations support a file:// URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The NETCONF <copy-config> operation supports using a file:// URI when <url> is the target and specifies the absolute path of a local file.

  [See <copy-config>.]

Platform and Infrastructure

- **DDoS syslog messages enhancement (MX Series devices with MPC10, MPC11, LC4800, or LC9600? line cards)**—We've enhanced the severity of the DDoS module syslog messages ddos_get_vbf_ifl_from_flow_id and ddos_get_vbf_ifl_name in a subscriber management environment. In earlier releases, these syslog messages displayed incorrect messages in a subscriber management environment when you enable SCFD (suspicious control flow detection).

  [See Control Plane DDoS Protection Flow Detection Overview.]

- **Two-Way Active Measurement Protocol (TWAMP) server/reflector test traffic classified by the ingress filter was re-classified with the values configured on the host-outbound-traffic configuration statement (All Junos OS Evolved platforms; MX Series platforms with MPC10E, MPC11E, or JNP10K-LC9600 cards)**—We no longer re-classify the egress TWAMP traffic. We now maintain the same queue for the packets in the egress direction that the packets had in the ingress direction.PR1739935

- Previously, shaping of Layer 2 pseudowires did not work on logical tunnel interfaces. This has been fixed for all platforms except QX chip-based MICs and MPCs.

User Interface and Configuration

- **Viewing files with the file compare files command requires users to have maintenance permission**—The file compare files command in Junos OS and Junos OS Evolved requires a user to have a login class with maintenance permission.

[See Login Classes Overview..]

VPNs

- **Increase in revert-delay timer range**— The `revert-delay` timer range is increased to 600 seconds from 20 seconds.

  [See min-rate.]

- **Configure min-rate for IPMSI traffic explicitly**— In a source-based MoFRR scenario, you can set a min-rate threshold for IPMSI traffic explicitly by configuring `ipmsi-min-rate` under `set routing-instances protocols mvpn hot-root-standby min-rate`. If not configured, the existing `min-rate` will be applicable to both IPMSI and SPMSI traffic.

  [See min-rate.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for MX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

NOTE: The Junos OS 23.2R2 Release offer limited or no support for the subscriber-management user-plane mode feature category.

General Routing

- When a P or PE router is configured with inline active flow monitoring and MPLS template with tunnel-observation ipv4/ipv6 is used, there is a chance that some EoMPLS packets may be exported using mpls-ipv4 or mpls-ipv6 template instead of mpls template.PR1713728
- On linecards and platforms using AFT, (that is, MPC10, MX304, LC9600), the final accounting stop stats for filters with accurate accounting enabled for the subscriber would be zero.PR1734608
- On Junos OS MX304 and MX Series platforms with LC9600 linecards, with the current error handling mechanism upon receiving fatal error on Flexible pic concentrators(FPC), leads to disable both the Packet Forwarding Engine on a Physical Interface Cards (PIC) card and seen traffic impact.PR1765394
- EBGP sessions established over IPSEC tunnels might flap, if multihop configuration statement is not configured. PR1791196

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. TSB18251PR1568757

MPLS

- Traceroute in MPLS OAM may fail with unreachable in ECMP case when topology has multiple ecmp paths in each transit router. This is because destination address is not available. Destination address is computed using base address + bitmap index(available for that leg).Junos currently supports 64 bitvector size.Each transit ecmp legs consumes available bitmap indexes in the echo request packet. When all the bitmap indexes are consumed by the previous transit routers/ecmp legs, then for other ecmp legs bitmap indexes are not available hence multipath information tlv bitmap will be zero leading to unreachable issue as no destination address is available. Even RFC 8029 section 4.1 says full coverage is not possible as below, If several transit LSRs have ECMP, the ingress may attempt to compose these to exercise all possible paths. However, full coverage may not be possible. Hence this is an expected behavior.PR1699685

Open Issues

IN THIS SECTION

Learn about open issues in this release for MX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

EVPN

- A few duplicate packets might be seen in an A/A EVPN scenario when the remote PE device sends a packet with an IM label due to MAC not learned on the remote PE device, but learned on the A/A local PE device. The nondesignated forwarder sends the IM-labeled encapsulated packet to the PE-CE interface after MAC lookup instead of dropping the packet, which causes duplicate packets to be seen on the CE side. PR1245316

General Routing

- If a vmhost snapshot is taken on an alternate disk and there is no further vmhost software image upgrade, the expectation is that if the current vmhost image gets corrupted, the system boots with the alternate disk so the user can recover the primary disk to restore the state. However, the host root file system and the node boots with the previous vmhost software instead of the alternate disk. PR1281554
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- runt, fragment and jabber counters are not incrementing on EX4300-MPsPR1492605
- IPSec rekey fails when SRX is configured with kilobyte based lifetime in remote access solution. PR1527384
- The Sync-E to PTP transient simulated by Calnex Paragon Test equipment is not real network scenario. In real network deployment model typically there will be two Sync-E sources (Primary and Secondary) and switchover happens from one source to another source. MPCE7 would pass real network SyncE switchover and associated transient mask PR1557999
- VE and CE mesh groups are default mesh groups created for a given Routing instance. On vlan/ bridge-domain add, flood tokens and routes are created for both VE and CE mesh-group/flood-group. Ideally, VE mesh-group doesn't require on a CE router where IGMP is enabled on CE interfaces. Trinity based CE boxes have unlimited capacity of tokens, so this would not be a major issue. PR1560588
- Due to a race condition, the 'show multicast route extensive instance instance-name" output can display the session status as Invalid. Such an output is a cosmetic defect and not indicative of a functional issue. PR1562387
- On EX2300, EX3400,:EX4300-48MP and EX4300 , Pause frames counters does not get incremented when pause frames are sent.PR1580560
- When the active slave interface is deactivated, the PTP lock status is set to 'INITIALIZING' state in 'show ptp lock-status' output for few seconds before BMCA chooses the next best slave interface. This is the day-1 behavior and there is no functional impact. PR1585529
- Pim Vxlan not working on TD3 chipsets enabling VxLAN flexflow after release 21.3R1. Customers Pim Vxlan or data plane VxLAN can use the Junos OS release 21.3R1. PR1597276
- output of show network agent command should be null, which shows statistic per component after GRES. PR1610325
- Percentage physical-interface policer is not working on AE, after switching between baseline config to policer config PR1621998

- The mspmand daemon running on MS-MPC/MS-MIC cards can occasionally crash when the service card (fpc/pic) is turned offline and then online at regular intervals when the number of service-set configured is moderately high and when extensive hardware crypto operations are being performed. Exact issue is yet to be isolated.PR1641107
- Please do not enable host-path tracing when there is high volume of packets been received in the host-path.PR1645741
- Multiple vulnerabilities have been resolved in MQTT (Message Queuing Telemetry Transport) included with Junos by fixing vulnerabilities found during external security research. Please refer to https://supportportal.juniper.net/JSA71655 for more information.PR1651519
- An Improper Neutralization of Equivalent Special Elements vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows a unauthenticated, adjacent attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA75741 for more information.PR1653316
- If the physical link status of the ethernet link between the RE and FPC goes down, there are recovery attempts to bring up the link again. Log messages indicate the recovery attempts and the success/failure status of the attempt. However an alarm is not raised when this failure occurs. Affects MX304 platform onlyPR1664592
- On MX Series platforms with MIC-MACSEC-20GE, Forwarding Engine Board (FEB) might go down while activating and deactivating GRES configuration.PR1668983
- On SyncE over LAG interfaces, if the end points have different ESMC QL configured, on one of configured syncE interface, ESMC QL is toggling between PRC and DNU and sync-E does not lock and moves to holdover state. PRC packets are received with MAC address of the upstream master. These packets are not dropped based on the link-local MAC address. Based on PLM recommendation inspired by the customer requirements and MEF 6.1.1 EPL Option 2 service (an excerpt below, taken from here https://www.mef.net/wp-content/uploads/2012/01/MEF-6-1-1.pdf) So, by default we are Option #2 compliant, if someone needs Option #1 behavior, a filter can be configured to match and discard. PR1677131
- A new command has been introduced that will display the differences between the destroute entries learned within l2ald and present in the kernelPR1677996
- There will be drop of syslog packets seen for RT_FLOW: RT_FLOW_SESSION_CREATE_USF logs until this is fixed. This will not impact the functionality.PR1678453
- On QFX5100 platforms (both stand-alone and VC scenario) running Junos, occasionally during the normal operation of the device, PFE (Packet Forwarding Engine) can crash resulting in total loss of traffic. The PFE reboots itself following the crash.PR1679919
- This fix supports single zone cooling(MX480:MX960:MX240). When one-third of time(240 sec) has past, chassisd brings down the FRU(FPC) which was causing over temp situation. If over temp

condition persists, timer will expire and whole chassisd will shutdown within 240 sec count down.PR1681716

- The issue here is that we see ?MQSS(0): DRD: Error: WAN reorder ID timeout error? once per PFE during bootup of FPC. This happens because during the FPC bootup some control packet from vmhost comes before the PFE init is fully complete. Because of this the EA Asic is not able to process the packet and throwing the error. The fix involves complex changes in the bootup sequence of ASICS and will result in other major issues. The original issue has no functionality impact. It is just one error per PFE seen during the FPC reload case only. At that time the traffic is not started yet and once the system is up no other impact is seen due to the Error. Hence the issue will not be fixed. Any "WAN reorder ID timeout error" during the bootup of FPC can be safely ignored.PR1681763
- For leaves of data type ieeefloat32, the value will be encoded in bytes while being streamed to collector. The value contained in such leaves may not be completely accurate.PR1690598
- Release note neededPR1697658
- Release note neededPR1697806
- FIPS mode is not supported in this release for SRXSME devices.PR1697999
- On MX platform, Once the device is loaded with the new image, PIC tries to boot up. mspmand is one of the processes inside PIC, crashes sometimes.PR1700462
- On MX platforms (with ukern based FPCs), dynamic VxLAN (PIM based) traffic convergence takes a little longer post ISSU.PR1703062
- When subscribing to sensor paths "/junos/system/linecard/packet/usage/", "/junos/services/label-switched-path/usage/" or other line card (PFE) sensor paths in gNMI subscription mode, packet drops may be seen in the CLI command "show network-agent statistics gnmi detail" output. The collector output may also contain missing sequence numbers. For example, the sequence number output may be 0, 3, 6, 9, 12, etc. instead of 0, 1, 2, 3, 4, etc.PR1703418
- Release note neededPR1703807
- The packets with internal ip address 128.0.0.xx -> 128.0.0.1 and upd port 2000 might be forwarded out the default egress interfaces. Such packets are telemetry data for PFE fabric sensor, which should be sent to routing-engine only.PR1706155
- When deleting a service-sets configuration, the Packet Forwarding Engine might restart on MX Series platforms with Multiservice-Modular Port Concentrator (MS-MPC). This leads to traffic loss. PR1706171
- In Chassisd, Junos Telemetry interface thread takes more time in streaming of Junos Telemetry interface packets because of volume of data and number of sensors involved with this daemon. Jvision thread engaged for more time to process streaming events caused Chassisd master thread to lose receive/send keepalive messages to/from other Routing Engine, which eventually was causing

automatic Routing Engine switchover in most of the cases. To avoid this, fix done for exporting small payload jvision packets (formation of which takes less time) and deferring jvision thread more in an interval, to allow chassisd master thread to process high-priority hello/keep-alive messages. This means now, more number of packets is sent in one reporting interval and with larger spread (earlier same amount of data was sent with 2 or 3 packets of higher payload size, and 100ms of deferring time for jvision thread. This behaviour is increasing KPI-2 but lowering KPI-1 (payload size). It is not possible to back out changes done to solve keep-alive message loss issue. Hence we will have to keep Chassisd as an exception, when we measure/report KPI-2 values. Jvision in Chassisd has to give more priority/time to process keep-alive messages than sending of jvision packets. Hence delay between jvision packets are more.PR1706300

- Current stack and display is correctly set to 128 ports that is qualified on all MX10K8 linecardsPR1706376
- When LAG is configured with mixed speed interfaces switching to a secondary interface of different port speed, results in a few packet drops for a very short duration. PTP remains lock and there is no further functional impact. PR1707944
- 1PPS and 2Way TE does not meet class B performance for 400G ports on JNP10K-LC9600 MPC. PR1709075
- On Junos OS and Junos OS Evolved platforms, the Dense Concentrator Packet Forwarding Engine (dcpfe) process crash will be observed due to memory fragmentation issue. This is a rare case and might impact traffic as due to dcpfe failure the Packet Forwarding Engine restarts, so the interfaces will flap.PR1711860
- The commit notification from 'edit private' mode won't produce correct patch.PR1713447
- Release note neededPR1713626
- On the MX104 platform, the Wrong threshold-temperature is displayed.PR1713788
- PRPD installed flowspec routes were not deleted on routing-instance delete, leading to RPD crash.PR1715599
- fec-codeword-rate data with render type decimal64 is rendered as string in grpc python decoder.PR1717520
- The requirement is to logout all subscribers on a port that will be further used in an SGRP, as config commit will not flag the existent subscribers for this port.PR1719297
- Segmentation fault on grpc timer thread (might be related to keepalive) #32085 grpc issue https://github.com/grpc/grpc/issues/32085 grpc stack needs to be upgraded to 1.53 or later.PR1722414
- In Subscriber Management, adding or deleting subscriber groups and subscriber group tags with one commit operation might generate an authd process core file. PR1722802

- The issue is related to the help syslog "^PFE_?" command tried on the configuration mode. As of now in some of the ERR_MSG tags are not listed when this command is triggered. This issue does not affect any functionality, but the impact is some of the Error message tags used are not listed when 'help syslog' command is used.PR1732668
- 400g option is visible under "set chassis fpc 0 pic 0 port port_num speed" command. For example: # set chassis fpc 0 pic 0 port 20 speed ? Possible completions: 100g Sets the interface mode to 100Gbps 10g Sets the interface mode to 10Gbps 200g Sets the interface mode to 200 Gbps 25g Sets the interface mode to 25Gbps 400g Sets the interface mode to 400Gbps 40g Sets the interface mode to 40Gbps 50g Sets the interface mode to 50GbpsPR1734654
- With a two-color policer configured on Aggregate Ethernet interfaces, the "queue-counters-trans-bytes-rate" counter may display an incorrect value.PR1735087
- On all Junos devices, the time needed to commit increases when a Trusted Platform Module (TPM) is configured.PR1738193
- On MX Series Virtual Chassis, because of the timing issue, when you restart the device, RPD will not spawn again. This issue is rarely reproducible.PR1740083
- On Junos OS Evolved ACX platforms with GRES (Graceful Routing Engine switchover), after performing GRES switchover jdhcpd doesn't start on the new master RE (Routing Engine) due to which DHCPv4/v6 (Dynamic Host Configuration Protocol) session binding will be lost resulting in traffic loss.PR1740530
- On MX Series platforms with MS-MPC/MS-DPC, when the system is busy in the creation/deletion of sessions results in the picd process crashes for executing the CLI command "show service sessions/flows" or "clear service sessions/flows" aggressively (executing CLI command in 5-10 secs iteration).PR1743031
- [TIMING BITS] - LOS alarm not generating when BITS is in LOS state. PR1744419
- On all Junos platforms with dual RE, error message: 'Minor potential slow peers are: X' will be seen. Due to some reason the PFE/PIC will be slow and services will face latency issue. the peerbuf list gets full, peer proxy could not enqueue further IPCs (ifstate chain/peer update to backup gets stalled) causing pfe/pics to be a slow consumer, this impacts service on the device. PR1747077
- On Junos using afeb/tfeb way of communication to PFE that is MX80/MX104 platforms with Virtual Router Redundancy Protocol (VRRP) configured, deleting a member link from the Aggregated Ethernet (AE) bundle removes the VRRP filter entry in the Packet Forwarding Engine (PFE) which causes VRRP traffic to get dropped even though other active member links in the AE bundle exists.PR1747289
- On MX104 platform with MACSEC MIC, the 'per-unit-scheduler' configuration on the MACSEC MIC interface results in the PFE crash leading to traffic impact.PR1747532

- On Junos QFX/EX platforms, the Packet Forwarding Engine (PFE) crash is observed while applying the firewall filters.PR1750828
- Mx304 the primary Routing Engine reports core-spmbpfe and secondary Routing Engine reports core-lcmd. PR1752639
- On MX2020, MX2010, MX10K4, and MX10K8 platforms and MPC11E, LC9600, LC4800 line cards, linecard loses all fabric planes (no links active) and takes all interfaces down when another linecard is powered off ungracefully .PR1762114
- Continuous reads can be performed by the control plane server side in some situations even when the external entity or client has closed the connection. This can cause increased control plane process CPU utilization.PR1765417
- On MX Series platform with a combination of MPC1-9, LC480, LC2101, and MPC10E, MPC11E, LC9600 line cards, when preserve-nexthop-hierarchy configuration statement enabled and maximum-ecmp configured with more than 32 next-hops in the MPLS fast-Reroute (MPLS-FRR) and BGP multipath scenario, packet loss when primary path is added back in ECMP nexthop (say after primary interface or session is marked UP) will be higher compared to that on MX Series platform with MPC1-9, LC480, LC2101 line cards only, OR with MPC10E, MPC11E, LC9600 line cards only. This packet loss is proportional to the value in maximum-ecmp configuration.PR1765856
- This error is only seen during corner case when you upgrade unified ISSU with scale configuration. The unified ISSU command still completes successfully even with this error. .PR1765931
- For certain releases, performing unified ISSU on MPC10 or MPC11 might generate an FPC core file. PR1766307
- SFB3 could go offline due to "[FATAL] Tx Async FIFO Underflow INTR for ZFIO" interrupt happened during SFB3, ADC, MPC7E links initialization. PR1768592
- On all Junos OS and Junos OS Evolved MX Series platforms, it is observed that when EVPN-MPLS and Preserve-nexthop-hierarchy are configured, then the address-resolution protocol (ARP) resolution fails and impacts the MPLS header packets that are sent to the MPLS core.PR1776913
- On MX Series platforms the "vxlan-gpe source-udp-port-range" feature is not working as expected leading to a traffic drop at the destination node if it validates the source port range.PR1781948
- If a PFE ASIC has a fatal fault leading to PFE Disable, there is a possibility that Fabric REQ Timeout logs may continue to flood the log messages for that PFE even though the PFE is no longer doing any traffic. These log messages can be ignored, but they will result in the **/var/log/** message file being rotated frequently.PR1788846

High Availability (HA) and Resiliency

- On Junos OS platforms, when ISSU (in-service software upgrade) is initiated, a process called INDB (Incompatible Database) will be triggered to perform a pre-check on database compatibility. There could be some corner case that causes the INDB crash. If that happens, the ISSU should be aborted.PR1740744
- The configuration of a private route doesn't support GRES, such as fxp0, when imported into a non-default instance or logical system. As a workaround, resolution rib policy is required. See KB26616. PR1754351

Interfaces and Chassis

- You can configure the routing platform to track IPv6-specific packets and bytes passing through the router. To enable IPv6 accounting, include the route-accounting statement at the [edit forwarding-options family inet6] hierarchy level: [edit forwarding-options family inet6] route-accounting; By default, IPv6 accounting is disabled. If IPv6 accounting is enabled, it remains enabled after a reboot of the router. To view IPv6 statistics, issue the `show interface statistics` operational mode command. PR717316
- Logical interface counter has a counter named "IPv6 transit statistics". It can be confirmed on `show interfaces extensive` command output. However, this counter is originally for IPv6 total statistics(transit + local) and the counter name was wrong from the first. On older releases like 19.1R1, as the support for IPv6 local stats was not available the local statistics was always zero. So, the meaning of the counter name was the same to the counting content coincidentally. In latest releases support for IPv6 local stats has been added but the counter name was not changed. As the local stats will not be zero the difference between the meaning of the counter name and the counting content started being visible. PR1631200
- On all Junos OS platforms, if a speed mismatch happens in the link aggregation (LAG) and member interface then a traffic drop will be seen.PR1725168
- On platforms like mx204, in case of near-end loss in SLM, "Near-end loss" percentage in CLI or jnxSoamLmCurrentStatsBackwardAvgFlr in SNMP will show very high, out of range values.PR1754637

Layer 2 Ethernet Services

- On MX104 platforms, when Active-Lease Query (ALQ) enabled with Dynamic Host Configuration Protocol (DHCPv6) relay agent configuration, ALQ syncing for DHCPv6 Transmission Control Protocol connection will not work due to issues while processing the ALQ messages and TCP handshake messages at peer.PR1727624

Layer 2 Features

- in a H-VPLS network with VPLS hot-standby and the configuration statement `routing-options forwarding-table vpls-hotstandby-convergence` enabled on spokes, if the active hub is rebooted, 20-25 seconds loss for inter-zone traffic stream is seen. This is due to hubs in other zones connected by full-mesh ldp, starting global repair before spokes starting local repair.PR1699645
- On Junos OS and Junos OS Evolved platforms in the VPLS multi-homing with multicast snooping enabled, the multicast traffic looping will be observed due to L2 (Layer 2) Multicast traffic being sent on the access interface status marked as CCC-DOWN.PR1774580

MPLS

- Tag rnh appears to be freed somewhere in the corner case, but the relevant pat node has been missed to delete from the tag patricia tree. That makes tag rnh/(pat_node->Tnh) a dangling pointer and later on, it results in a crash while accessing invalid pointer addresses in the tag rnh/Tnh structure.PR1707053
- Trace route in MPLS OAM on SR over IPv6 may fail in ECMP case if EVO box is in topology. This is because linux kernel in EVO puts an auto flow label on every IPv6 packet. This flow label is transparent to daemon process, which uses a null value for it and calculates the NH details. PFE however takes the flow label into account and calculates the NH details. This difference in calculation of NH details leads to a mismatch in the path the packet takes to the destination and can cause trace route to fail.PR1710285
- LDP sync not complete with NSR (stuck at Inprogress forever) when "protocols ldp strict-targeted-hellos" is enabled when LDP signalled VPLS is configured.PR1725519

Network Management and Monitoring

- In some NAPT44 and NAT64 scenarios, Duplicate SESSION_CLOSE Syslog will be seen. PR1614358
- After upgrading the Junos OS on DUT, yang package with lower revisions are available in upgraded Junos OS version. PR1693646

Platform and Infrastructure

- When the `deactivate services rpm` and `deactivate routing-options rpm-tracking` configuration statements are applied together and then committed, some of the rpm tracked added routes are not deleted from the routing table. Issue cannot be seen using the following steps. 1. deactivate routing-options rpm-tracking 2. commit the configuration then all the rpm tracked routes will be deleted. If the RPM service needs to be deactivated, 3. deactivate services rpm 4. commit. PR1597190
- MVPN RVT MX EA cards: RVT interface traffic statistics are not proper. PR1755516
- R1 which is in DF forwards BUM traffic to CE where only DF PE is supposed to forward. PR1757314

Routing Policy and Firewall Filters

- Auto export feature requires a target tree to be created for it to function. This target tree is created when an exporter has an export policy with that target configured under "then" clause and an importer has that target configured under the "from" clause. Without this target tree, the route will not be exported. Say we have a situation where an instance 'VRF-1' with auto export configured has a route with a target and an importer 'VRF-2' has a policy accepting this route. 1) VRF-1 will not export the route unless its export policy has that target community configured under "then" clause. 2) Let us assume VRF-1 does not have the target community configured under "then". So the target tree is not created. Now let us assume another instance VRF-3 has an export policy with that community configured under "then". Now, VRF-1 will export that route to the VRF-2. This is why it is inconsistent. If VRF-1 wants to export the route, a config change in VRF-3 should not suddenly allow the export to happen.PR1745957

Routing Protocols

- Certain BGP traceoption flags (for example, "open", "update", and "keepalive") might result in (trace) logging of debugging messages that do not fall within the specified traceoption category, which

results in some unwanted BGP debug messages being logged to the BGP traceoption file. PR1252294

- LDP OSPF are in synchronization state because the IGP interface is down with ldp-synchronization enabled for OSPF. user@host> show ospf interface ae100.0 extensive Interface State Area DR ID BDR ID Nbrs ae100.0 PtToPt 0.0.0.0 0.0.0.0 0.0.0.0 1 Type: P2P, Address: 10.0.60.93, Mask: 255.255.255.252, MTU: 9100, Cost: 1050 Adj count: 1 Hello: 10, Dead: 40, ReXmit: 2, Not Stub Auth type: MD5, Active key ID: 1, Start time: 1970 Jan 1 00:00:00 UTC Protection type: None Topology default (ID 0) -> Cost: 1050 LDP sync state: in sync, for: 00:04:03, reason: IGP interface down config holdtime: infinity. As per the current analysis, the IGP interface goes down because although LDP notified OSPF that LDP synchronization was achieved, OSPF is not able to take note of the LDP synchronization notification, because the OSPF neighbor is not up yet. PR1256434

- On MX Series platforms, unexpected log message will appear if the CLI command `show version detail` or `request support information` is executed: test@test> show version detail *** messages *** Oct 12 12:11:48.406 re0 mcsnoopd: INFO: krt mode is 1 Oct 12 12:11:48.406 re0 mcsnoopd: JUNOS SYNC private vectors set PR1315429

- On all Junos and Junos Evolved platforms, the rpd (routing protocol daemon) can crash when PIM (Protocol Independent Multicast), MoFRR (Multicast only Fast Reroute) configuration is present and some network churn event such as continuous interface cost changes, resulting in a change of active and backup paths for ECMP (Equal Cost Multi-Path) happens. There will be service impact because of the rpd crash but the system self-recovers until the next crash.PR1676154

- Errors might be seen on ephemeral commit during ISSU.PR1679645

- BGP LU statistics does not report correct statistics when sharding is enabled. PR1684238

- On all Junos OS and Junos OS Evolved platforms, whenever a commit is done, that involves mcsnoopd daemon config parsing such as (VLAN creation/deletion, interface add/delete to VLAN, interface enable/disable, IGMP (Internet Group Management Protocol) snooping/MLD (Multicast Listener Discovery) snooping related config commands) mcsnoopd will consume CPU. In less scaled setup (few IGMP snooping enabled VLANs and few hundred IGMP snooping memberships), the CPU time taken is less. In a more scaled setup (many IGMP snooping-enabled VLANs and a few thousand IGMP snooping memberships), the CPU may reach >90%. Since mcsnoopd is taking high CPU, it may affect other daemons like rpd. It may affect all the protocols if the CPU is not available to the protocols/daemons. This can impact route entries expiring and cause traffic drop.PR1710565

- Egress statistics are not seen on Junos Telemetry interface sensor configured over the segment routing. PR1700063

- On all platforms, high rpd CPU utilization might be observed when a routing related commit is performed in a high-scaled environment having BGP groups configured with VPN family (inet-vpn, inet6-vpn). No traffic impact or protocol flap will be seen but unexpected high rpd CPU utilisation will raise operational challenges, especially if the system is very scaled.PR1728829

- On all Junos OS and Junos Evolved platforms, with BGP Monitoring Protocol (BMP) configured when a BGP peer import policy configuration change is committed that triggers the BGP reconfiguration job for routes re-evaluation, then high Routing Protocol Daemon (rpd) CPU utilization up to 100% will be observed for a long time which may impact routing as high rpd utilization can starve some processes.PR1729733

VPNs

- On all Junos OS and Junos OS Evolved platforms with dual Routing Engine and Multicast Virtual Private Network (MVPN) enabled, when the user initiates a GRES, it triggers a route change from the MVPN . During this process, there's a gap where traffic loss is observed because the flood next hop pointed to the route gets deleted.PR1747703
- Additional ipmsi-min-rate option provided as part of existing min-rate to configure separate rate for IPMSI, if configured. If not configured, the existing min-rate will be applicable for both IPMSI and SPMSI.PR1788769

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for MX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Class of Service (CoS)

- The change in forwarding-class via OpenConfig will not work as expected. PR1726298
- The CoS scheduler map will not get attached to the sub-interface correctly when shaping-rate and scheduler-map are configured on it PR1734013
- "load override" followed by ISSU will introduce incorrect class-of-service FC (Forwarding Class)-to-Q(queue) table mapping. PR1755540
- Change in the cosd behaviour due to the CoS interface specific wildcards. PR1760817
- Duplicate code points through code-point-aliases under a classifier results in cosd crash. PR1766873

EVPN

- [NPI Templeton] [Supportability] - Macros for EVPN/VXLAN traces. PR1692769
- ARP learning issues are observed post-execution of the CLI command `clear bridge mac-table` or `clear ethernet-switching table` in the EVPN-MPLS over IRB environment. PR1718165
- SRv6 locator change results in rpd crash. PR1724845
- EVPN-VXLAN interconnection DCI forwarding problem was observed when one of the AGW IRB interfaces failed in data centers spine. PR1732414

- While doing a migration from VPLS to EVPN, when any changes are done like FPC restart or device reboot, the crash is observed PR1734686
- ARP/FIB are added even if IRB in EVPN is disabled. PR1743529
- The user will be unable to configure the interface having stacked outer VLAN and a list of inner VLANs. PR1746787
- Intermittent packet loss can be observed in evpn-vpws local switching scenario. PR1747706
- The rpd can crash on all Junos OS platforms in seamless DCI scenario. PR1761852
- [EVPN/MPLS] Color related LSPs for next-hop will disappear from EVPN routes on mpls.0 routing-table by changing `fallback none` option in `transport-class` configuration. PR1764126

Forwarding and Sampling

- Traffic not hitting the policer after configuring macroflow filter. PR1718147
- FPC cards restart unexpectedly. PR1743032
- High CPU utilization of the mib2d process will be observed with error messages due to stale SNMP requests PR1749092
- Traffic loss observed when using ingress-queuing-filter on non zero Packet Forwarding Engine interface. PR1751494

General Routing

- Inter vlan IPv6 traffic loss for some hosts after configuration remove and restore. PR1629345
- Delegated BFD sessions configured on routing-instance may fail to come up. PR1633395
- Earlier to Junos OS release 22.2R1S2 can be installed on RE-S-X6-128G-K. This will result in system booting to Linux prompt. PR1655935
- Continuous error logs and telemetry data might not be populated. PR1661423
- Logical interface packet counters do not work on show AMS interface extensive for sub interfaces. PR1673337
- The PFE will get disabled for underrun cmerrors observed when traffic ingressing over the AF interface. PR1681428

- VTEP is getting resolved over EM0 - log an error if this happens. PR1688296
- xml validation failure seen for "show security macsec connections | display xml validate" with ERROR: Duplicate data element. PR1691435
- RPC "get-bgp-group-information' execution failure with WARNING and CRITICAL ERROR. PR1698030
- MFT: RPD may restart during Multi-Feature-Test with BGP-MP, L3VPN/L2VPN, over RSVP/LDP transport, as well as colored SRTE, and SRv6 tunnel transport along with BGP CT. PR1699773
- Alarms for PEMs are still seen when PEM are removed from the chassis. PR1703566
- Interface flaps are seen after PTP GM changes to a different FPC slot. PR1704633
- No alarm is raised when PSU is inserted with different airflow directions. PR1710952
- Subscribers connectivity is lost due to multiple MIC restart on all Junos OS MX Series platforms with MPC5E and BBE configuration. PR1713968
- VMX: Total LSP count mismatch on path computation client after PCCD restart. PR1714158
- The agentd would become unresponsive on all Junos OS platforms. PR1715377
- Traffic leak is seen during a filter change. PR1715504
- BMP station will not receive the RIBs as expected. PR1715886
- Traffic loss due to incorrect route resolution and KRT queue getting stuck with 'EINVAL -- Bad parameter in request' error. PR1716436
- J-flow sends wrong IP in sampling records when NAT is configured for traffic along with input sampling. PR1716707
- Same MAC address is assigned to cbp and physical interfaces instead of being unique on MX304. PR1719084
- The subscribers will be stuck in a terminated state when an FPC is taken offline. PR1719427
- Continuous messages indicating duplicate IP address L2ALM_DUPLICATE_IP_ADDR will be seen in MCLAG and VRRP scenario. PR1719868
- Removing a PEM that doesn't have power feed does not generate the SNMP TRAP for "Power Supply Removed". PR1719915
- Reachability loss between Master and backup RE in certain condition on MX2008 platform PR1720407

- The bbe-statsd process crash is observed on the backup RE immediate after GRES was disabled. PR1720978
- Unnecessary power is consumed as the SFP laser will still be on even though the port is down/ disabled. PR1720998
- Local route is not added in the secondary FIB on all Junos SRX platforms and routes will be permanently stuck in KRT queue. PR1721032
- L2alm sends IPv6 NS with IRB link local address even though target IP is global address. PR1722102
- The filter will not work as configured upon changing the "physical-interface-policer" parameters. PR1722776
- The FPC crash is observed on Junos MX10008 platform when connected to non-Juniper SFP. PR1722823
- PADT response will not be sent for an incoming PPPoE/PPP data Packet from an unknown session ID. PR1722945
- PS interface remains up while LT or RLT interface is down. PR1724298
- Help string "Display information for a specified VLAN" is changed to "Display information for a specified bridge domain". PR1724489
- The IDS session-limit is not allowing new sessions even though the sessions are under the limit. PR1724626
- Traffic loss will be observed with vlan tagging and/or vlan normalisation in a specific design (using a looped cable) PR1724675
- gNMI native Junos configuration push commit fails if configuration has special character. PR1724746
- Memory initialization and scrub operation using PFE's fails. PR1724841
- The entPhysicalSoftwareRev MIB object returns Junos OS version value for components which do not run Junos OS. PR1725078
- The "show network-access address-assignment address-pool-manager status command" reports APM not connected when in fact it is connected PR1725143
- DCPFE process crash can be seen on all Junos EX and QFX5K platforms with MACSEC enabled. PR1725375
- The error logs "fpc0 expr_hostbound_packet_handler: Receive pe 254?" are generated. PR1725716
- Delete notifications for sub-interfaces missed in gRPC telemetry. PR1726205
- Root user is unable to login using public key authentication after reboot or upgrade. PR1726621

- Upgrading the i40e NVM Firmware on Routing Engines with VM Host Support. PR1726775
- The EVPN-VXLAN proxy-arp will respond with the wrong MAC when no-mac-learning is configured. PR1727119
- On all Junos and Junos Evolved platforms the l2ald process memory usage is seen to increase over time. PR1727954
- The tunnel remains down and traffic is impacted due to no validation of the tunnel forwarding route. PR1728305
- Multiple NTP vulnerabilities resolved. PR1729126
- When there is a power outage happens after the first upgrade, the reboot device gets stuck at volume booting. PR1729671
- Traffic drops are observed on MX Platform configured with PCP mapping along with NAT. PR1729801
- DHCP subscribers are stuck in DHCP-Renew state when 'overrides always-write-giaddr' is enabled. PR1729913
- Packets received on a port that is in "LACP Detached" state is getting forwarded. PR1730076
- 'max-db-size' configuration is optional in routers having DRAM greater than or equals to 32GB. PR1732216
- Incorrect gNOI "Rotate" and "Install" gRPC stream handling. PR1732601
- Traffic drop will be observed when RIPv2 is enabled on IPv4 interface. PR1732673
- [PDT][MX304] xmlproxyd coredump was seen when running gnmi collector. PR1732763
- The Junos Selective Upgrade (JSU) version is not removed post a major Junos upgrade/downgrade. PR1732878
- Error logs are seen with a non-vxlan dot1x enabled port. PR1733365
- Traffic loss is seen when "lacp force-up" knob is configured. PR1733543
- IPsec traffic drops when two ARI routes get installed for the same tunnel. PR1734212
- Junos OS: jkdsd crash due to multiple telemetry requests (CVE-2023-44188). PR1734718
- The bbe-smgd crash can be seen in a certain scenario. PR1735560
- Control plane flap, data drop, unexpected behavior of PFE or device is observed when file storage is impacted in a continuous ksyncd process crash scenario. PR1735685

- Crash on all Junos VMhost platforms due to deadlock panic. PR1735843
- Unexpected VLAN tagging behavior would be observed in the EVPN-VXLAN scenario. PR1736954
- BGP session flaps due to license updates. PR1737035
- The traffic silently drops or discards when the SRTE shortcut is configured. PR1737119
- Traffic drop can be seen in the MPLS traffic Engineering scenario. PR1737594
- URL-Filtering few HTTP sites are getting bypassed and redirect is not happening. PR1737670
- IPv4 leaf elements for ps transpfort ifl are exported, since ps is l2 interface no statistics under IPv4 should be exported. PR1737935
- Eventd running 100 percent CPU cycle while running AMS statistics related show command continuously. PR1738300
- JV DB is missing leaf: /interfaces/interface[name=\'ae0\']/state/counters/out-octets , out-pkts, out-unicast-pkts , out-broadcast-pkts , out-multicast-pkts , in-errors , out-errors, in-discards ,out-discards ,in-pause-pkts, out-pause-pkts PR1738395
- PTP time sync issues after release upgrade or rebooting the device. PR1738458
- DHCP offer is dropped at MX and specific EX platforms when an lt interface is used as the transport. PR1738548
- An rpd crash will be observed due to inconsistency between rpd and kernel. PR1738820
- The ksyncd process crash would be seen on backup Routing Engine. PR1739258
- Memory leak in PKID. PR1739342
- The FPC will core and crash in a race condition. PR1739595
- Major alarms will be observed on the FPC when ALB is enabled under AE interface. PR1739854
- FPC crashes and remains offline after the upgrade of RE BIOS to 0.15.1 version. PR1739922
- Layer 2 traffic will be dropped on VSTP disabled interface. PR1739975
- Traffic loss is seen due to anomalies after the recreation of IFLs. PR1740561
- The traffic drop is observed due to the MAC source address being learned from the wrong direction. PR1741316
- The BGP routes gets stuck in BMP withdraw state. PR1741732
- SPMB process will crash and PICs will not come online. PR1742186

- Tunnel interfaces are getting bounced causing a momentary impact on traffic. PR1742510
- Race condition where FLOOD ROUTE DEL event can cause l2ald crash. PR1742613
- JUNOS_REG:MX240:Illinois:Traffic verification failed for DHCPv6 relay PR1743087
- The l2ald crashes when there is recursive deletion of IFBD or when BGP neighborship is cleared in EVPN-VXLAN multi-homed configuration. PR1743282
- The chassisd crash is observed on Junos MX204 platforms due to Fabric request timeout. PR1743379
- Due to SPMB restarts in the middle of the FPC boot process, FPC wont come up. PR1743686
- The switch-options settings on the logical-system will be not reflected after RE rebooting or RE switchover. PR1743737
- If more than 32 vlan ranges are configured under the dynamic-profile then login issue and traffic impact can be seen with subscribers of random VLANs PR1743903
- Traffic drop is observed after the addition or removal of the "filter-specific" knob under the policer PR1743930
- GRE over IPv6 will not work resulting in traffic impact post-upgrading the device PR1743978
- [USF - SPC3 - LOGGING] "log-tag" is not populated in the cgnat syslogs intermittently PR1744563
- With multiple Traffic Selectors having same remote-ip, the traffic works only for first tunnel on MX platforms with SPC3 cards PR1744601
- 100G interfaces will flap due to RE switchover on Junos MX platforms with MPC3E-3D-NG/ MPC-3E-3D-NG-Q linecards PR1744883
- Fans may stop working after removal and insertion of Fan Tray PR1745299
- MPC10E - PIC bounce/config change on a PIC with 10G QSA adaptor can cause a FPC restart PR1745317
- Packet drops may be seen in the "show network-agent statistics detail" CLI output when subscribing to sensors using gRPC PR1745451
- rpd core at #2 0x00007f9b2512742c in __assert_fail_base (fmt=0x7f9b2528bae8 "%s%s%s:%u: %s %sAssertion `%s' failed.\n%n", assertion=0x55be37507a48 "nh_idx_t_getval(nhid) == nh_idx_t_getval(rt_nexthops_nhid(rtnh))", file=0x55be375077e8 "../../../../../../../../src/layer3/ usr.sbin/rpd/lib/krt/common/krt_ack.c", line=1306, function=optimized out) at assert.c:92. PR1745509
- The rpd crashes when BGP sharding, multipath and dynamic tunnel are configured PR1746012

- Node-segment reachability will be lost in multitopology based IS-IS. PR1746304
- MPC10E line card crashes when it reboots after FPC firmware upgrade. PR1746541
- PTP master feature will not work as expected PR1746984
- Traffic from subscribers will be dropped by Junos based MX Series platforms. PR1747009
- MX204 - INLINE NAT - address-prefix any-ipv4 reporting wrong. PR1747483
- Packet drop will be observed due to ARP resolution failure in EVPN-VXLAN scenario PR1747878
- Frequent fabric plane Check state reported due to remote destination timeouts PR1747893
- The memory consumption increases due to memory leak PR1747992
- The rpd process shuts down on all Junos and Junos OS Evolved platforms PR1749252
- Connectivity fails intermittently on 802.1x enabled ports PR1749312
- PFE Flow ID doesn't shows correct in "show subscriber extensive" output PR1749336
- Router crashes if routing services over PS are configured PR1749748
- The authentication algorithm hmac-sha-256-128 for IPsec SA is not working and causing interoperability issues between Junos Evolved platforms and other devices PR1749779
- IRB interface state remains up on local-remote option on all platforms along with EVPN-VxLAN configuration PR1750146
- SyncE stuck in holdover upon PTP slot switchover without change in PTP phase align state PR1750316
- MX304: ssh is not enabled by default. PR1750596
- Traffic transfer/receive is impacted for SPC3 CPU cores connected to the affected PCIe bus when the SPC3 card boots up PR1750634
- The mspmand daemon crashes causing traffic loss PR1750823
- MPC10E: Support of G.8275.1 PTP Hybrid mode with speed 25G and 400G PR1750885
- ARP learning issue for dynamic ARP entry for the DVLAN stacked frame route not resolved PR1751656
- Incorrect egress MTU errors when larger than 1500 byte packets are sent on L2 ports PR1751700
- FPC reboots observed during ISSU on MX10008/MX10016 resulting in ISSU being unsuccessful PR1751785

- Service PIC enabled with url-filtering may crash and gets into booting loop PR1751860
- Firmware upgrade will fail, if "set system services ssh root-login deny" knob is present in configuration PR1752765
- Incorrect egress encapsulation corrupting packets of IRB interface on MPC10E with MXVC results in traffic loss PR1753951
- Traffic impact will be seen for static VoIP VLAN on access interface if same VLAN configured as data VLAN PR1754474
- "set services evpn global-parameters virtual-gateway v6-mac" is broken PR1754493
- Users authenticated via captive portal experience a noticeable delay of atleast 2-5 mins PR1755593
- Continuous fpc0-aftd-trio coredump on MX304 when turning up ipv6 neighbors with LMIC 2 PR1755950
- HMC errors will be observed on Junos OS platforms with LC480 PR1756780
- Interface using QSA adapter with 1G speed wont work after upgrade to 21.4R3-S4.9 PR1757878
- On JNP10K-LC9600, shared-bandwidth-policer may be loaded into irrelevant PFE depending on choice of member port of aggregated Ethernet. PR1758935
- LLDP neighborship will not be formed on all Junos devices PR1763053
- BFD session detection time is higher than expected leading to traffic drop PR1763667
- High RPD CPU due to BMP station config PR1764911

High Availability (HA) and Resiliency

- The traffic drop is observed during the Graceful restart on Junos and Junos Evolved platforms PR1727957

Interfaces and Chassis

- Physical link remains stuck in down state on certain MX Series platforms PR1707707
- The interface speed gets set to a lower speed when the interface is disabled and enabled because renegotiation of the interfaces happens at the previously negotiated speed PR1714267

- Traffic loss due to PFE table not getting updated when new VLANs are added in an AE bundle under ESI configuration PR1726073
- The lt/vt/ut interfaces may not recover from the disable-pfe (admin down) state if the GRES switchover is done before restarting FPC PR1731190
- High memory utilization is observed on all Junos OS platforms PR1757801

Junos Fusion Satellite Software

- Junos Fusion Satellite device will be stuck in the SyncWait state PR1733558

Layer 2 Ethernet Services

- DHCP binding is not happening in EVPN VXLAN topology with DHCP stateless relay (forward-only) PR1722082
- DHCP ALQ no-advertise-routes-on-backup functionality does not work in VRF for Framed-Route. PR1740822
- Active bulk leasequery is not working for IPv6 DHCP local server on MX Series platforms PR1744162

Layer 2 Features

- The rpd crash is seen due to the creation of a new logical interface PR1680687
- The rpd process crash will be observed during VPLS to EVPN migration PR1729052

MPLS

- The rpd process crash is observed when RSVP LSP at Juniper transit/ingress router receives RESV message with RESVCONF object in multi vendor deployment PR1723229
- Traffic silently drops due to an additional label when CCNH is toggled PR1738774

- LSP with auto bandwidth enabled is not updating its Max AvgBW value, preventing the LSP from being resized PR1740226
- rpd crash observed during RE switchover or Route Convergence PR1747365
- In-place-lsp-update failure causing ungraceful tear down of LSP PR1756096

Network Management and Monitoring

- Syslog messages modification for SNMPv3 authentication failure PR1734549

Platform and Infrastructure

- Inbound traffic will be blocked if the FPC is restarted when there is a continuous input traffic PR1602741
- VRRP does not work when a firewall filter is configured to accept VRRP packets with a TTL value of 255 PR1701874
- ksyncd core with dhcp subscribers PR1722708
- Traffic loss observed for packets over IRB over LT PR1724925
- Syslog severity of ddos_get_vbf_ifl_from_flow_id and ddos_get_vbf_ifl_name messages is incorrect PR1727005
- Multiple CFM sessions are down when vlan rewrite feature is configured on AE interfaces PR1727049
- VPLS traffic gets blackholed by qualified-bum-pruning mode PR1731564
- Heap memory leak on MPCs used for subscriber termination. PR1732690
- Intermittent flooding of traffic every 40 seconds. PR1736667
- The CoS rewrite rules will not be working in the EVPN with IRB scenario PR1736890
- MPC1 to MPC13E/LC2101,LC2103,LC480/T4000-FPC5/MPC built-in Trio based line card reboots when subscriber management services are configured PR1737615
- Host communication does not work in EVPN-L2VPN-CCC setup PR1740606

- Inline-monitoring will not work as expected when more than one instances are configured PR1742123
- show system connections show-routing-instances; reports all routing-instances as unknown. PR1746779
- M/MX: Ksyncd cores are seen after performing Restart routing, with replication error PR1752151
- TCP window scaling may be not applied to the first TCP packet sent to the client after the three-way handshake, leading to unnecessary segmentation. PR1761242
- Routing Protocol session down with native VLAN configuration on MX platforms PR1763706
- afeb core file is generated with heap high. PR1770750

Routing Policy and Firewall Filters

- Policy change to a rib-group import-policy configured with global routing-options interface-routes causes the rpd issue on all platforms with EVPN-VXLAN configuration PR1744449

Routing Protocols

- The mscnoopd process crash is observed when snooping configuration is removed PR1696374
- The mcscnoopd process get stuck in resync state after snooping configuration is deleted and added again immediately PR1699784
- Junos OS and Junos OS Evolved: A crafted BGP UPDATE message allows a remote attacker to de-peer (reset) BGP sessions (CVE-2023-4481) PR1709837
- The PE advertises incorrect next-hop towards CE although BGP export policy configured with next-hop under policy-statement PR1712527
- RPD process crashes on all Junos and Junos OS Evolved platforms after adding static route to the VRF in some scenarios PR1720240
- The rpd process crash is observed when TI-LFA feature is enabled PR1723172
- Unnecessary SPF calculation is causing high CPU utilization PR1725686
- The rpd process crashes when BGP is cleaned up PR1728455
- Traffic loss is seen due to BGP sessions stuck in 'openconfirm' state PR1728508

- The RPD process will be stuck at a high CPU when OSPF areas are configured at a high scale and after starting the protocol PR1728573
- Traffic impact is seen when there is a single peer in the proxy BGP group connected to the BGP route reflector PR1728604
- The rpd will crash upon receiving a malformed BGP UPDATE message (CVE-2023-44204) PR1731803
- The rpd process will crash in a scaled BGP setup with traceoptions configured PR1732087
- The rpd process crash will be observed with BMP and independent resolution is enabled for secondary BGP routes PR1732493
- The adjacent PE Node SID label will drop from routing table when MicroLoop-Avoidance is enabled in OSPF-SR PR1732500
- Constant BGP peer flaps and rpd core file is generated. PR1732833
- Junos OS and Junos OS Evolved: RPD crash when attempting to send a very long AS PATH to a non-4-byte-AS capable BGP neighbor (CVE-2023-44186) PR1736029
- The rpd crash files are seen due to a use-after free of objects PR1737679
- OSPFv3 using the VIP address on the IRB interface will not form adjacencies between peers PR1737978
- BFD session for BGP remains down in a specific scenario PR1738074
- RPD crashes when multiple ISIS processes are configured PR1738222
- Traffic loss will be seen in IPv6 only IS-IS topologies PR1738901
- The rpd process crash will be observed when the prefix-limit exceeds on the backup RE PR1739335
- The IPv6 link local based BFD session over an AE interface will be stuck in Init state PR1739860
- Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute (CVE-2023-0026) PR1739919
- Error message for mld static group configuration is not proper. PR1741370
- Memory leak observed when reconfiguring the flow routes PR1742147
- Partial application of BGP import policy with BMP configuration and after back-to-back commits changes BGP import policy PR1742222
- RPD scheduler slip is observed when the BGP session flaps and subsequent configuration changes for the same peer PR1742416

- When BGP is configured in routing-instance of type virtual-router, default MPLS table is being created for that virtual-router, unexpectedly PR1742513
- CPU in rpd spikes and scheduler slips will be observed when the duplicate community is added PR1745073
- Traffic loss observed in SR-LDP stitch scenario when ECMP is enabled on PTX platforms PR1746349
- Route-distinguisher change leads to the route being present in rpd, but not installed in kernel/PFE PR1746439
- Stale IP prefixes when issuing "show isis route flex-algorithm-id" PR1746557
- With RIB sharding configuration upon rpd restart the rpd crash will be observed PR1748152
- Multi-instance isis route leaking for inet.3 is not working as expected PR1748223
- The device will not be reachable over the loopback interface for the IS-IS nodes even though the neighborship may exist PR1749850
- RPD may crash when deactivate protocol ISIS PR1751210
- ISIS export policy does not export all default routes (IPv6 and IPv4) from BGP (or any other protocol) PR1751371
- Traffic drop is seen if chained-composite-next-hop is turned on for Segment Routing PR1752551
- The rpd crashes on all Junos and Junos Evolved platforms with IS-IS, segment routing and flex algo configured PR1753003
- BGP multipath route is not correctly applied after changing the IGP metric PR1754935
- The BGP LU labels can have next-hops pointing to each other in multi-homed PE setup PR1760885
- Memory spike will be observed on the system with BFD enabled for OSPF/ISIS PR1761232

Services Applications

- L2TP tunnels may time out if creation of bbe-smgd core dump takes a long time. PR1720994
- Crash file is generated when local certificate keychain is missed repeatedly PR1728605

Subscriber Access Management

- Subscriber sessions will fail to login post GRES and scaled subscriber scenario PR1723183
- Potential memory leak in authd process PR1729035
- Test aaa command may failure due to "Subscriber creation failed" PR1759048

User Interface and Configuration

- After the device reboot BGP sessions will be down PR1726731
- Device boots up even with incompatible configuration PR1730442
- The mgd process will crash due to stack overflow on high scale address configuration PR1741413

VPNs

- MVPN tunnel is not synced to backup router PR1710323
- Junos OS: Multiple Vulnerabilities in CLI command (CVE-2023-44178). PR1723674
- In MPLS-L2VPN/BGP-VPLS setup the flow-label route update is not propagating to neighbouring devices. PR1751717

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading to Release 23.2R2

NOTE: 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
```

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 (the only exceptions are the juniper.conf and ssh files might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see the Installation and Upgrade Guide.

For more information about the installation process, see Installation and Upgrade Guide and Upgrading Junos OS with Upgraded FreeBSD.

Procedure to Upgrade to Junos OS

To download and install Junos OS:

1. Using a Web browser, navigate to the All Junos Platforms software download URL on the Juniper Networks webpage:

   https://www.juniper.net/support/downloads/

2. Select the name of the Junos OS platform for the software that you want to download.
3. 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.
4. Select the Software tab.
5. In the Install Package section of the Software tab, select the software package for the release.

6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new jinstall package on the routing platform.

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.

All customers except the customers in the Eurasian Customs Union (currently composed of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package:

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-23.2R2.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-23.2R2.9-signed.tgz
```

Customers in the Eurasian Customs Union (currently composed of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package (Limited encryption Junos package):

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-23.2R2.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-23.2R2.9-limited.tgz
```

Replace source with one of the following values:

- */pathname*—For a software package that is installed from a local directory on the router.
- For software packages that are downloaded and installed from a remote location:
  - **ftp://** ***hostname/pathname***
  - **http://** ***hostname/pathname***
  - **scp://** ***hostname/pathname***

Use the `reboot` command to reboot the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process might take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

NOTE:

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.
- Starting in Junos OS Release 21.1R1, in order to install a VM host image based on Wind River Linux 9, you must upgrade the i40e NVM firmware on the following MX Series routers:
  - MX240, MX480, MX960, MX2010, MX2020, MX2008, MX10016, and MX10008

  [See https://kb.juniper.net/TSB17603.]

NOTE: Most of the existing `request system` commands are not supported on routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. See the VM Host Software Administrative Commands in the Installation and Upgrade Guide.

Upgrading a Router with Redundant Routing Engines

If the router has two Routing Engines, perform the following Junos OS installation on each Routing Engine separately to avoid disrupting network operation:

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine, and save the configuration change to both Routing Engines.
2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.
3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.
4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

For the detailed procedure, see the Installation and Upgrade Guide.

Downgrading from Release 23.2R2

To downgrade from Release 23.2R2 to another supported release, follow the procedure for upgrading, but replace the 23.2R1 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 4: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

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

Junos OS Release Notes for NFX Series

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for the NFX Series.

To view features supported on the NFX Series platforms, view the Feature Explorer using the following links. To see which features are supported in Junos OS Release 23.2R2, click the Group by Release link. You can collapse and expand the list as needed.

- NFX150
- NFX250
- NFX350

What's Changed

Learn about what changed in this release for NFX Series devices.

Known Limitations

There are no known limitations in hardware or software in this release for NFX Series devices.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Open Issues

IN THIS SECTION

Learn about open issues in this release for NFX Series devices.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- On the NFX platforms, when one partition supports a Junos OS Release 23.4R1 image (supported on LTS19 operating sytem) and the other partition supports an image older than Junos OS Release 23.4R1 (supported on WRL8 operating system), the `request vmhost reboot disk` command is not executed as expected.

  As a workaround, upgrade both the partitions with same image versions PR1753117.

Virtual Network Functions (VNFs)

- On NFX150 devices, before reusing a VF to Layer 3 data plane interfaces (for example, ge-1/0/3), which was earlier allocated to a VNF, you must restart the system. PR1512331

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for NFX Series

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Interfaces

- On Junos NFX350 Platforms, if you disable any RJ-45 interface through configuration, auto-negotiation at the MAC (Media Access Control) level on the remaining ports of the group of 4 ports (either 0-3 or 4-7) is disabled, resulting in traffic disruption. The impact isconfined to the group of ports on which the port is disabled and the other group is not affected.

  PR1731242

VNFs

- On Junos NFX350 Platforms, in spite of disabling the Auto Negotiation (AN) on the interface through configuration, it stays enabled on the copper ports.This could result in mismatch of AN settings with the remote side configuration and disrupt traffic.

  PR1719973

- Non-root user cannot access VNF through SSH, Telent, and console.

  PR1756270

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

NOTE: For information about NFX product compatibility, see NFX Product Compatibility.

Basic Procedure for Upgrading to Release 23.2R1

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

NOTE: 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 device, such as configuration templates and shell scripts (the only exceptions are the juniper.conf and ssh files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the device. For more information, see the Software Installation and Upgrade Guide.

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 download and install Junos OS Release 23.2R1:

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks webpage:

   https://www.juniper.net/support/downloads/

2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the **Software** tab.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list to the right of the Download Software page.
5. In the Install Package section of the Software tab, select the software package for the release.
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. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the device or to your internal software distribution site.
10. Install the new package on the device.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 5: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

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

Junos OS Release Notes for QFX Series

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for QFX Series switches.

To view features supported on the QFX platforms, view the Feature Explorer using the following links. To see which features are supported in Junos OS Release 23.2R2, click the Group by Release link. You can collapse and expand the list as needed.

- QFX5110
- QFX5120-48Y
- QFX5120-32C
- QFX5120-48T
- QFX5120-48YM
- QFX5200
- QFX5210-64C
- QFX10002
- QFX10008
- QFX10016
- QFX10002-60C

What's Changed

IN THIS SECTION

Learn about what changed in this release for QFX Series Switches.

EVPN

- **EVPN-VXLAN tracing configuration**— The `set services trace evpn-vxlan` configuration invokes a built-in commit script to generate tracing configurations for troubleshooting EVPN-VXLAN in multiple modules and hierarchies.

  See [trace (EVPN-VXLAN).]

- **Default behavior changes and new options for the easy EVPN LAG configuration (EZ-LAG) feature**— The easy EVPN LAG configuration feature now uses some new default or derived values, as follows:

  - Peer PE device `peer-id` value can only be 1 or 2.

  - You are required to configure the loopback subnet addresses for each peer PE device using the new `loopback-subnet peer1-subnet` and `loopback peer2-subnet` options at the `edit services evpn device-attribute` hierarchy level. The commit script uses these values for each peer PE device's loopback subnet instead of deriving those values on each PE device. The `loopback-subnet` option at the `edit services evpn device-attribute` hierarchy level has been deprecated.

- If you configure the `no-policy-and-routing-options-config` option, you must configure a policy statement called EXPORT-LO0 that the default underlay configuration requires, or configure the new `no-underlay-config` option and include your own underlay configuration.
- The commit script generates **notice** messages instead of **error** messages for configuration errors so you can better handle `edit services evpn` configuration issues.
- The commit script includes the element names you configure (such as IRB instance names and server names) in description statements in the generated configuration.

This feature also now includes a few new options so you have more flexibility to customize the generated configuration:

- `no-underlay-config` at the `edit services evpn` hierarchy level—To provide your own underlay peering configuration.
- `mtu overlay-mtu` and `mtu underlay-mtu` options at the `edit services evpn global-parameters` hierarchy level —To change the default assigned MTU size for underlay or overlay packets.

[See Easy EVPN LAG Configuration.]

- **Limit on number of IP address associations per MAC address per bridge domain in EVPN MAC-IP database**—By default, devices can associate a maximum of 200 IP addresses with a single MAC address per bridge domain. We provide a new CLI statement to customize this limit, `mac-ip-limit` statement at the **edit protocols evpn** hierarchy level. In most use cases, you don?t need to change the default limit. If you want to change the default limit, we recommend that you don?t set this limit to more than 300 IP addresses per MAC address per bridge domain. Otherwise, you might see very high CPU usage on the device, which can degrade system performance.

  See [mac-ip-limit.]

General Routing

- Before this change most list were ordered by the sequence in which the user configured the list items, for example a series of static routes. After this change the list order is determined by the system with items displayed in numerical sequence rather than by the order in which the items were configured. There is no functional impact to this change.
- While running `request system snapshot recovery` command on all VMHost based Routing Engines, disable or stop reporting any warning message.
- **Autonegotiation status in show interfaces extensive output (QFX5120-48Y):** The `show interfaces extensive` output shows the autonegotiation information for SFP-T transceivers.

- **Media type in show interface extensive command (QFX5210-64C)**— The media type shows ?Fiber? in the `show interface et-x/y/z` command output for optics transceivers.

  See [**show interfaces extensive**.]

- **New commit check for MAC-VRF routing instances with the encapsulate-inner-vlan statement configured**— We introduced a new commit check that prevents you from configuring an IRB interface and the `encapsulate-inner-vlan` statement together in a MAC-VRF routing instance. Please correct or remove these configurations prior to upgrading to 23.2R2 or newer to avoid a configuration validation failure during the upgrade.

  See [encapsulate-inner-vlan.]

- NOTE: In the CLI using the command request chassis feb slot slot-number offline if you make the primary FEB offline, a traffic loss warning message is displayed and the FEB offline request is rejected. If offline/restart is still intended for primary FEB, use force option in addition to the command. WARNING message displayed in the CLI: "warning: RCB and FEB work in the paired slot mode. FEB %s offline/restart will result in traffic loss and does not cause a switchover. Please re-try after initiating a mastership switchover using 'request chassis routing-engine master switch' CLI. If offline/restart is still intended, use 'force' option in addition to this CLI."

- **Change in options and generated configuration for the EZ-LAG configuration IRB subnet-address statement**—With the EZ-LAG `subnet-address inet` or `subnet-address inet6` options at the `edit services evpn evpn-vxlan irb` *`irb-instance`* hierarchy, you can now specify multiple IRB subnet addresses in a single statement using the list syntax **addr1 addr2 ?**. Also, in the generated configuration for IRB interfaces, the commit script now includes default `router-advertisement` statements at the **edit protocols** hierarchy level for that IRB interface.

  [See subnet-address (Easy EVPN LAG Configuration).]

- Media Access Control Security (MACsec) session remains stable when changing exclude-protocol configuration—When you change the protocols excluded from MACsec using the exclude-protocol protocol-name option at the `edit security macsec connectivity-association connectivity-association-name`, the MACsec session remains stable.

  [See exclude-protocol.]

- **ChaCha20-Poly1305 algorithm deprecation for SSH cipher option** — The ChaCha20-Poly1305 authenticated encryption algorithm is deprecated for SSH cipher option. Configure aes-128-gcm and aes-256-gcm as the encryption algorithm for SSH Cipher option.

  ssh (System Services)

Interfaces and Chassis

- Starting in Junos OS release 23.2R1 and Junos OS Evolved release 23.2R1-EVO, the output of show chassis power command displays the state of the power supply in PTX10003 and QFX10003 platforms.

  See [show chassis power.]

- When all the members of the AE have the same speed (x) and no mixed speed configured. If you change the speed value of any member of the AE to a value other than x, the commit succeeded in earlier releases. From this release, the commit fails. When there are et interfaces with different speeds and you want them to be part of an AE interface. If you change the speed of all the members of the interfaces to be the same speed (x), configure the AE interface, and commit, the commit failed in earlier releases. From this release, such commits succeed.

Junos XML API and Scripting

- **Ability to commit `extension-service file` configuration when application file is unavailable**—When you set the `optional` option at the `edit system extension extension-service application file` *`file-name`* hierarchy level, the operating system can commit the configuration even if the file is not available at the **/var/db/scripts/jet** file path.

  [See file (JET).]

Network Management and Monitoring

- **NETCONF `<copy-config>` operations support a `file://` URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The NETCONF `<copy-config>` operation supports using a `file://` URI when `<url>` is the target and specifies the absolute path of a local file.

  [See <copy-config>.]

- **`ephemeral-db-support` statement required to configure MSTP, RSTP, and VSTP in the ephemeral configuration database (ACX Series, EX Series, and QFX Series)**—To configure Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), or VLAN Spanning Tree Protocol (VSTP) in the ephemeral configuration database, you must first configure the `ephemeral-db-support` statement at the `[edit protocols layer2-control]` hierarchy level in the static configuration database.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

Platform and Infrastructure

- Previously, shaping of Layer 2 pseudowires did not work on logical tunnel interfaces. This has been fixed for all platforms except QX chip-based MICs and MPCs.

Routing Protocols

- In Junos OS Evolved platforms, `show route snooping` and `show route forwarding-table` does not show /56 routes in the VPLS address family table.
- **Optimized mesh group routes (QFX5110, QFX5120, QFX5130, QFX5700 and ACX Series)**— `show route snooping` for inet.1/inet6.1 table and `show route snooping table inet.1/inet6.1` will display only CE mesh group routes for platforms that support EVPN-MPLS or EVPN-VxLAN multicast. In earlier releases, other mesh groups like the VE mesh group were also displayed.
- Starting in Junos OS Evolved 23.4R1, we have enabled the `process-non-null-as-null-register` configuration statement under `edit protocols pim rp local` by default. For earlier releases, you must configure this statement explicitly.

User Interface and Configuration

- **Viewing files with the `file compare files` command requires users to have `maintenance` permission** — The `file compare files` command in Junos OS and Junos OS Evolved requires a user to have a login class with `maintenance` permission.

  [See Login Classes Overview.]

VPNs

- **Increase in revert-delay timer range**— The `revert-delay` timer range is increased to 600 seconds from 20 seconds.

  See [min-rate.]

- **Configure min-rate for IPMSI traffic explicitly**— In a source-based MoFRR scenario, you can set a min-rate threshold for IPMSI traffic explicitly by configuring `ipmsi-min-rate` under `set routing-instances`

`protocols mvpn hot-root-standby min-rate`. If not configured, the existing `min-rate` will be applicable to both IPMSI and SPMSI traffic.

See [min-rate.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for QFX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- During software validation, Junos OS mounts the new image and validates the configuration against the new image. Since the TVP-based QFX platforms (QFX5000 and QFX10000) are already mounting the maximum 4 disks during normal execution it cannot mount the extra disk for this purpose. Thus QFX currently does not support configuration validation during upgrade on QFX5000 so the syntax error appears when the image installation is triggered with **validation**. PR1421378
- Higher than expected loss and traffic null routes are seen during node failures with node protection on FTI interfaces for RSVP LSPs. PR1456350
- PFC is not supported across the FPCs with the HGOE VCPs.PR1709186
- Dot1x daemon read the configuration whenever there is change in time based license for the feature macsec. PR1713881
- This is a third-party limitation and Day 1 issue affecting third-party chipsets such as EX4650's, QFX5000s, EX4300. One VLAN can be mapped to only on ERPS ring. For example, VLAN 100 can be mapped to only one ERPS ring. This same VLAN 100 cannot be part of another ERPS ring on the same switch. PR1732885

- This is a vendor limitation and Day 1 issue affecting vendor chipsets such as EX4650's, QFX5000s, EX4300. One VLAN can be mapped to only on ERPS ring. For example, VLAN 100 can be mapped to only one ERPS ring. This same VLAN 100 cannot be part of another ERPS ring on the same switch.PR1732885

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the **no-validate** option to complete successfully. PR1568757

Open Issues

IN THIS SECTION

Learn about open issues in this release for QFX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- Pim VXLAN not working on TD3 chipsets enabling VXLAN flexflow after release 21.3R1. Customers Pim VXLAN or data plane VXLAN can use the version 21.3R1. PR1597276

- QFX5100-24Q devices VC (Virtual-chassis) is in unstable state for 3-7 minutes causing traffic loss. PR1661349
- When the remote end server and system reboots, QFX5100 platform ports with SFP-T 1G inserted might go into a hung state and remain in that state even after the reboot is complete. This might affect traffic after the remote end system comes online and resumes traffic transmission. PR1665800
- When the power cable is removed or inserted, **jnxPowerSupplyFailure and jnxPowerSupplyOK** might not be generated on backup FPC. PR1667952
- On QFX5100 platforms (both stand-alone and VC scenario) running Junos OS, occasionally during the normal operation of the device, PFE (Packet Forwarding Engine) can crash resulting in total loss of traffic. The PFE reboots itself following the crash. PR1679919
- On Junos QFX5100 and EX4600-Virtual Chassis (VC) and Virtual Chassis Fabric (VCF) platforms on upgrading Virtual Chassis Fabric (VCF) and toggling the interface, when FPC (Flexible PIC Concentrators) is disabled and rebooted, the member fails to join the virtual chassis and the interface remains disabled even after been enabled. PR1689499
- When TISSU upgrade is done from 22.4 release onwards, the box come up as backup Routing Engine. Work-around:- To make is primary following command needs to be run again. sysctl -w hw.lc.issuboot=0 sleep 10 sysctl -w hw.re.issu_state=0 sleep 10 sysctl -w hw.re.tissu=0 sleep 10 sysctl -w hw.product.pvi.config.chasd.no_re_status_on_backup=1 sleep 60. PR1703229
- The `show chassis hardware` indicates duplicate entries for PSU and FAN tray after USB clean install or zeroize. PR1704106
- On Junos OS and Junos OS Evolved platforms, the dcpfe (Dense Concentrator Packet Forwarding Engine) process crash will be observed due to memory fragmentation issue. This is a very rare case and would impact traffic as due to dcpfe failure the PFE restarts, so the interfaces will flap. PR1711860
- On EX4650 and QFX5120-48Y, the SFP-LX interface will not be UP when different Small Form-factor Pluggable(SFP-10GBASE-T and SFP-LX) are plugged in within the same 4 port group. The presence of the 10GE-T SFP resets the speed of the quad back to 10G even if the quad port speed is set to 1G. Normally 10G interface by itself will be up when set to 1G if no other SFP is plugged in. PR1714833
- In a VC of QFX5100-24Q with an expansion module EX4600-EM-8F, if VC is formed on 10G ports then after the reboot of VC, the 10G connections will be lost and the line card will show as not present. This will impact traffic on the 10G ports after connection is lost. PR1718062
- On the Junos QFX5200 platform, sometimes 100G link will go down and will remain down. PR1725116

- On QFX5000 platforms with QSFP+-40G-ACU10M and Virtual Chassis configured, traffic loss will be observed due to CRC (Cyclic redundancy check) errors. PR1729067
- This problem is seen on QFX10000 platform, when ingress Sflow is enabled on bridged AE (tagged) interfaces and that incoming traffic gets forwarded through IRB interfaces on an ECMP path. In ECMP scenario, Sflow injects TAL request into the ASIC which are resulting in the traps tracked through this PR. Hence the forwarding traffic is unaffected. PR1729316
- On QFX5100 platforms error occurs while configuring packet-forwarding-options. PR1730451
- When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted might go into a hung state and remain in that state even after the reboot is complete. This might affect traffic after the remote end system comes online and resumes traffic transmission. PR1742565
- In a QFX51200-48YM-8C VC setup, after a primary switch over fan tray of linecard might not be displayed in `show chassis hardware` and `show chassis environment`. There is no functional impact. PR1758400
- When there are a large number of aggregated (AE) interfaces on a system, deleting all of them together and adding them back can lead to a race condition. This could result in a few of the interfaces not being programmed correctly. PR1781955

High Availability (HA) and Resiliency

- Graceful Routing Engine Switchover (GRES) not supporting the configuration of a private route, such as fxp0, when imported into a non-default instance or logical system. PR1754351

Interfaces and Chassis

- Following two failure messages seen brcm_rt_ip_mc_ipmc_install:2455 Failed (Invalid parameter:-4) This message is due to IPMC Group being used is not created, when RE tried to add this check indicates there is a parameter mis-match. brcm_rt_ip_mc_ipmc_install:2455 Failed (Internal error:-1) This message is due to failure to read IPMC Table or any memory/register. PR1461339
- On all Junos OS platforms, if a speed mismatch happens in the LAG (Link Aggregation) & member interface then a traffic drop will be seen. PR1725168

Layer 2 Ethernet Services

- On QFX5100 and QFX5110, vendor-id format maybe incorrect for network ports. This does not impact the ZTP functionality or service. The DHCP client configuration is coming from two places, that is AIU script and VSDK sandbox. The DHCP client configuration coming from AIU script has the serial ID in vendor ID where as the default configuration from sandbox does not have. PR1601504

Virtual Chassis

- On Junos OS, QFX5100 platforms running QFX-5e images in Virtual Chassis setup, when Virtual Chassis Port (VCP) links are connected between PHY and PHYLESS ports, CRC alignment errors will be seen. As a result, there can be traffic loss on these links. PR1692102
- With SR4 optics on QFX5210 some times we can see partial continuous traffic drop observed on IPv4 and IPv6 streams (framing errors). PR1785882

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for QFX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- Traffic drop would be observed along with the error message **Buffers are stuck on queue** when performing the OIR in the 100G QSFP interface. PR1641572
- Traffic is not restored when Layer 2 circuit configurations are deleted and added back on QFX5000. PR1666260
- Minor packet drops due to hardware programming issues. PR1700927
- Port-mirroring state remains down on Junos QFX5000 platforms. PR1705015
- No alarm is raised when PSU is inserted with different airflow directions. PR1710952
- The dcpfe process crash is seen on QFX5000 platforms due to stale vtep entry. PR1712175
- QSFP-100G-LR4-T2 optics will stay down after ISSU/TISSU. PR1713010
- The dot1x-protocol subsystem is not responding to management requests while verifying in show security mka sessions. PR1713881
- Traffic null-route after reboot. PR1714701
- IGMP/MLD queries might get dropped if received on a port on the backup VC member when IGMP/MLD snooping is enabled. PR1716902
- Layer 2 Multicast traffic drops when PIM is configured without IGMP Snooping enabled. PR1720527
- FPC crash on QFX5120-48Y. PR1721297
- Error message is generated when DHCP packet is received through remote VTEP. PR1721318
- Momentary traffic loss is observed when interface with local Type-2 ESI goes down. PR1722348
- QFX10000 not bridging multicast traffic with TTL=1 on same VLAN. PR1723433
- ECMP traffic is not being forwarded on all QFX10002 platforms after software upgrade. PR1723545
- Traffic loss will be observed with VLAN tagging and/or VLAN normalisation in a specific design (using a looped cable). PR1724675
- The error logs **fpc0 expr_hostbound_packet_handler: Receive pe 254?** would be generated. PR1725716
- The class of service subsystem crashed after the device is restarted or the switchover is performed. PR1726124
- Delete notifications for sub-interfaces missed in gRPC telemetry. PR1726205

- On QFX5120-48y-8c platform 10G ports go down in a port group if 25G SFP is inserted in the same group. PR1726707
- The EVPN-VXLAN proxy-arp will respond with the wrong MAC when no-mac-learning is configured PR1727119
- Configuration load failure from event script fails on QFX5100-48S-6Q after upgrading to 21.4R3. PR1727834
- On all Junos OS and Junos OS Evolved platforms the l2ald process memory usage is seen to increase over time. PR1727954
- The tunnel remains down and traffic is impacted due to no validation of the tunnel forwarding route. PR1728305
- QFX debugging command `show aq107 xxx` on VTY might generate an error on 10GBASE-T SFP if AQ index exceeds 48. PR1728452
- The dcpfe process core observed after restarting the l2-learning process with flex-hashing configuration. PR1729101
- Sflow sampling will not work on Junos OS based QFX10000 platforms. PR1729316
- The fpc detaching logs will be seen when the VC port between different FPCs are flapped. PR1729647
- Packets received on a port that is in **LACP Detached** state is getting forwarded. PR1730076
- Traffic is impacted due to high CPU and dcpfe/fxpc crash (in some cases) in EVPN-VXLAN scenario. PR1730771
- DCPFE/FXPC process crash could be observed on all Junos QFX5000 platforms with EVPN-VXLAN configuration. PR1731212
- Traffic for VLAN-ID 2 gets dropped in Ethernet-CCC Layer 2 Circuit on QFX5000 platforms. PR1731291
- Traffic drops when any of the VXLAN VLAN is deleted. PR1731583
- QFX5000 : Error message 'LBCM-L2,pfe_bcm_stp_set_nostp_port_state(),X:handling for lag with no members[op x ifd aeX vid x]' is seen when changing config related to interface. PR1732217
- SNMP polling Timeout due to OID 1.3.6.1.2.1.31.1.1.1.10.514 (ifInOctets.514). PR1732708
- On router reboot an interface in SP style blocks all packets on **family inet/inet6** interfaces if VSTP is configured on VLAN-bridge encapsulated VLANs. PR1732718
- QFX5120 reboots due to deletion of EP style interface with native VLAN configured. PR1733022

- Traffic loss is seen when `lacp force-up` configuration statement is configured. PR1733543
- Online SIBs will go down due to a faulty SIB that triggers spmbpfe crash. PR1734734
- Packet drop is observed due to SIB ASIC issue on fabric. PR1734735
- BFD session remains stuck in INIT state on certain QFX platforms. PR1736348
- [timing] [ptp] QFX5120-48YM 1PPS Performance measurement test fails. PR1736385
- Unexpected VLAN tagging behavior would be observed in the EVPN-VXLAN scenario. PR1736954
- Link down due to FEC mismatch on Junos OS based QFX5000 platforms using 25G-LR optics. PR1738077
- Null-route of l3-inject traffic on QFX10000 platforms. PR1738197
- Traffic drop observed when encapsulation ethernet-bridge is configured on the aggregate Ethernet interface associated with VxLAN VLAN. PR1738205
- High convergence time in the EVPN-VxLAN uplink failover scenario. PR1738276
- Multicast will not work if one or more VLANs are removed from the interface having multicast configured. PR1738355
- [QFX5/EX] Error message like BRCM-VIRTUAL,brcm_vxlan_port_discard_set(),13034:Failed to set bcm_port_discard_set to 0 for port (61) err(Invalid unit). PR1738404
- An rpd crash will be observed due to inconsistency between rpd and kernel. PR1738820
- DSCP classifier is not created on IP interfaces. PR1738981
- Q-in-Q for access port to access port through VxLAN bridge-domain does not work on all Junos QFX5000 platforms. PR1739048
- The ksyncd process crash would be seen on backup Routing Engine. PR1739258
- QFX5120-48Y : The information of auto negotiation on SFP-T is not displayed. PR1739808
- The loop-detect is not working in the VXLAN scenario. PR1740327
- Traffic loss is seen due to anomalies after the recreation of IFLs. PR1740561
- The traffic drop is observed due to the MAC source address being learned from the wrong direction. PR1741316
- Enabling sflow triggers ddos-protection violation of protocol group resolve. PR1741461
- SPMB process will crash and PICs will not come online. PR1742186

- Traffic dropped is observed in the MPLS LDP scenario when the peer device MAC address is changing. PR1742364
- Race condition where FLOOD ROUTE DEL event can cause l2ald crash. PR1742613
- Traffic drop will be observed after extended-vni-list configuration change with EVPN-VXLAN scenario. PR1742763
- QFX52XX: check loop detect fails after Restart L2ald. PR1743083
- After ZTP process, the configuration fetch from the script path in event-options is impacted. PR1743222
- GRE over IPv6 will not work resulting in traffic impact post-upgrading the device. PR1743978
- BPDU Protection with packet-action drop support on QFX10002-60C. PR1745102
- The clear error command support for qfx10002-60c. PR1746244
- QFX10002-60c port et-0/0/30 part of a lag is dropping peer ARP reply after configuring a GRE tunnel. PR1746435
- [QFX5000]When RSI(request support information) is executed in the VC configuration, some errors output. PR1746788
- Due to timing issues, PFE/PICs will be slow and traffic will be impacted on all Junos OS platforms. PR1747077
- [QFX] Under rare situations, 10GBASE-T SFP might be unable to make the peer end deivce linkdown. PR1747277
- Alarm LED is lit due to LICENSE_EXPIRED on Virtual Chassis backup even with the valid license. PR1747720
- Packet drop will be observed due to ARP resolution failure in EVPN-VXLAN scenario. PR1747878
- Unable to install IPv6 routes in LPM table. PR1748462
- Traffic drop will be observed when Label MPLS traffic egressing out on the IRB interface as IPV4. PR1748500
- Deletion of duplicate MAC marked as BLOCKED MAC results in the l2ald crash. PR1748604
- Traffic drop can be seen when 'port' match is used for filtering on QFX5000 platforms. PR1749214
- L3VPN traffic destined for hosts learned over IRB/VXLAN will get dropped on QFX10000 platforms. PR1750468
- The PFE process crashed while removing and applying the firewall filters. PR1750828

- Incorrect egress MTU errors when larger than 1500 byte packets are sent on Layer 2 ports. PR1751700
- Traffic loss is observed for IPV6 streams sent between EVPN-VxLAN-L3VPN tunnel on Junos QFX10000 platforms. PR1754254
- QFX: VC(virtual chassis) does not get formed when using 100G for vc port. PR1754838
- [QFX5120]Egress filter does not work properly on VLAN pop configuration. PR1754929
- Layer 2 VXLAN and Layer 3 IPv4 Logical Interfaces are not getting configured on the same interface. PR1756407
- Learning stops in logical interface in QFX10000 platforms. PR1756672
- The dcpfe process crash will be seen when L2PT interfaces are configured with multiple protocols. PR1757329
- The ARP entry is not completed without the l3-interface part of the VLAN with proxy-arp/arp-suppression. PR1757364
- Multicast traffic drop observed when IGMP/MLD snooping is configured with IRB. PR1758659
- Generate an empty file whose name is secondary_vlan when executing RSI. PR1759875
- Traffic drop will be seen due to an incorrect VLAN tag. PR1760823
- On Junos OS and Junos OS Evolved platforms the rpd crashed abnormally and later chassisd crashed as well. PR1761667
- ECMP traffic drop after the aggregate Ethernet interface flap. PR1761887
- LLDP neighborship will not be formed on all Junos OS devices. PR1763053
- VPLAG information not installed correctly in hardware results in traffic flooding. PR1763116
- BFD session detection time is higher than expected leading to traffic drop. PR1763667
- LLDP neighborship is not forming in non-primary members. PR1764085
- The telemetry stops streaming data when the jsd CPU utilization goes high. PR1765344
- A warning message is seen while installing a license key with an unknown feature. PR1766515
- An unnecessary traffic load on the peer boxes. PR1767190
- Virtual chassis formation fails for VCP ports. PR1768554
- Data center interconnect configuration addition needs to be non-catastrophic. PR1769086

- Incorrect IFL value resulting in the PFE crash. PR1770678
- Memory leak observed on non-local FPC for Junos QFX5000 platforms. PR1771183
- Family ethernet-switching policer per-sub-unit interface breaks after dcpfe/device restarts. PR1771630
- BFD over Service Provider Style configuration of bridge Interface fail. PR1771651
- The PVST BPDU packet get dropped in transparent EVPN-VXLAN on the ingress PE-CE port of SP style on Junos QFX platforms. PR1771739
- The IP packet of Layer 2 Unicast MAC and Layer 3 undirected broadcast IP (255.255.255.255) is dropped when sent over an IRB interface. PR1771879
- Firewall filters will not work if IRB interface and layer 2 filter attached to BD is configured in SP style on QFX10000 platforms. PR1772126
- The tagged traffic drop will be seen with vlan-id-list and native-vlan-id configured on one IFL. PR1773676
- The dcpfe process crash due to stale memory. PR1774366
- QFX: fails to ping IPv6 link local address in routing instance if there is a default route in the same. instance. PR1775394
- The PVST (VSTP) UNTAGGED BPDU packet get dropped in transparent EVPN-VXLAN on the ingress PE-CE port of SP style on Junos QFX platforms. PR1775672
- The fxpc process crash is seen on a specific QFX platforms except EX4300 due to memory leak after VTEP IFLs configuration and un-configuration. PR1777265
- Traffic drop is observed when VIPs become unreachable due to GARP sent on VLANs to which the VIP does not belong. PR1778725
- At the interface level, only half of the traffic is policed when applying a policer. PR1779527
- On QFX10002-60c platforms, during system reboot and fpc reboot time, some non functional error logs are displayed. PR1779890
- With EVPN-VXLAN configured, when a Layer 3 interface or underlay IRB interface deletion results in a traffic null route. PR1781691
- Junos OS: Impact of Terrapin SSH Attack (CVE-2023-48795). PR1781732
- A few aggregate Ethernet interfaces will drop traffic when a large number of AE interfaces are deleted and added back. PR1781955

- MTU adjustment on Junos OD QFX5000 platforms with GRE Causes FPC and Link Partner FPC reboots. PR1782762
- The fxpc process crash and the device reboots after deleting Aggregated Ethernet (AE) interface along with its associated physical interface and then applying new interface configuration on the associated physical interface in an EVPN-VXLAN scenario. PR1783397
- Traffic loss after PIC restart if the packet has a VLAN tag of 4095. PR1788573

EVPN

- BUM (Broadcast, Unknown Unicast, and Multicast) Traffic can be dropped in some instances. PR1727054
- VLAN programming fails due to bridge domain change on QFX platforms. PR1739466
- EVPN-VXLAN comp nh is not installed in PFE after peer reboot. PR1739686
- After deactivating or activating GBP configuration in the MH AE scenario all tag entries not getting re-learned on leaf nodes in the ethernet-switching table resulting in traffic loss. PR1739878
- ARP/FIB are added even if IRB in EVPN is disabled. PR1743529
- IRB reachability issues may be observed in the EVPN-VXLAN environment when looped ARP comes on ESI-LAG. PR1743913
- Traffic discarded on QFX5000 platforms in multi-homed EVPN-VXLAN scenario. PR1749759
- Re-ARP is not sent before MAC entry expires in EVPN environment on Junos MX platforms. PR1751386
- Traffic flooding for MAC addresses programming failure. PR1758677
- Traffic is black-holed on QFX5000 platforms in EVPN-VXLAN scenario. PR1758783
- Traffic loss for few seconds will be observed after restarting l2-learning process on Layer 3 VxLAN gateway. PR1777635

Interfaces and Chassis

- Traffic impact will be seen with mismatched speeds on the LAG interface and member interface. PR1725168

- High memory utilization is observed on all Junos OS platforms. PR1757801
- Services using the management interface will be affected on all Junos OS platforms. PR1757936

Layer 2 Ethernet Services

- DHCP binding is not happening in EVPN VXLAN topology with DHCP stateless relay (forward-only). PR1722082
- The LAG with member interface enabled with 'force-up' can flap after switchover. PR1773827

MPLS

- The rpd crash observed during Routing Engine switchover or Route Convergence. PR1747365

Platform and Infrastructure

- The CoS rewrite rules will not be working in the EVPN with IRB scenario. PR1736890
- In EVPN-MPLS/EVPN-VxLAN Multi-Home Active/Active scenario, random packet drops are observed. PR1772733

Routing Policy and Firewall Filters

- Policy change to a rib-group import-policy configured with global routing-options interface-routes causes the rpd issue on all platforms with EVPN-VXLAN configuration. PR1744449

Routing Protocols

- The mcscnoopd process will be stuck in resync state after snooping configuration is deleted and added again immediately. PR1699784

- Junos OS: A crafted BGP UPDATE message allows a remote attacker to de-peer (reset) BGP sessions (CVE-2023-4481). PR1709837
- RPD process crashes on all Junos OS and Junos OS Evolved platforms after adding static route to the VRF in some scenarios. PR1720240
- Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute (CVE-2023-0026). PR1739919
- Memory leak observed when reconfiguring the flow routes. PR1742147
- Route-distinguisher change leads to the route being present in rpd, but not installed in kernel/PFE. PR1746439
- BGP multipath route is not correctly applied after changing the IGP metric. PR1754935

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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 QFX Series 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 Installation and Upgrade Guide and Junos OS Basics in the QFX Series documentation.

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

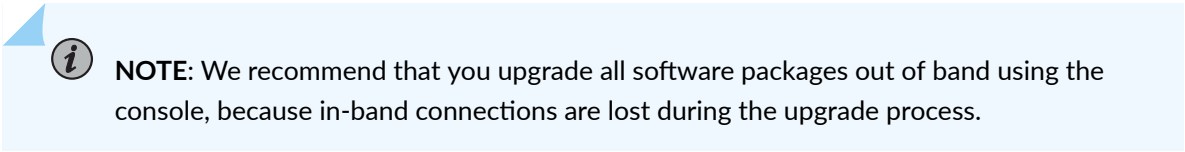
1. In a browser, go to https://www.juniper.net/support/downloads/junos.html.

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 **23.2** 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 20.3 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-host-qfx-5-x86-64-23.2-R1.n-secure-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 20.3 `jinstall` package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

This section explains how to upgrade the software, which includes both the host OS and the Junos OS. This upgrade requires that you use a VM host package—for example, a **junos-vmhost-install-*x*.tgz** .

During a software upgrade, the alternate partition of the SSD is upgraded, which will become primary partition after a reboot .If there is a boot failure on the primary SSD, the switch can boot using the snapshot available on the alternate SSD.

NOTE: The QFX10002-60C switch supports only the 64-bit version of Junos OS.

NOTE: If you have important files in directories other than /config and /var, copy the files to a secure location before upgrading. The files under /config and /var (except /var/etc) are preserved after the upgrade.

To upgrade the software, you can use the following methods:

If the installation package resides locally on the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-23.2R1.9.tgz
```

If the Install Package resides remotely from the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add ftp://ftpserver/directory/junos-vmhost-install-qfx-x86-64-23.2R1.9.tgz
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the `show version` command.

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

Installing the Software on QFX10002 Switches

NOTE: If you are upgrading from a version of software that does not have the FreeBSD 10 kernel (15.1X53-D30, for example), you will need to upgrade from Junos OS Release 15.1X53-D30 to Junos OS Release 15.1X53-D32. After you have installed Junos OS Release 15.1X53-D32, you can upgrade to Junos OS Release 15.1X53-D60 or Junos OS Release 18.3R1.

NOTE: On the switch, use the `force-host` option to force-install the latest version of the Host OS. However, by default, if the Host OS version is different from the one that is already installed on the switch, the latest version is installed without using the `force-host` option.

If the installation package resides locally on the switch, execute the **request system software add** ***<pathname><source>*** **reboot** command.

For example:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-f-x86-64-23.2R1.n-secure-signed.tgz reboot
```

If the Install Package resides remotely from the switch, execute the **request system software add** ***<pathname><source>*** **reboot** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-f-
x86-64-23.2R1.n-secure-signed.tgz reboot
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the `show version` command.

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

Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

The switch contains two Routing Engines, so you will need to install the software on each Routing Engine (re0 and re1).

If the installation package resides locally on the switch, execute the **request system software add** ***<pathname><source>*** command.

To install the software on re0:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-
domestic-signed.tgz re0
```

If the Install Package resides remotely from the switch, execute the **request system software add** ***<pathname><source>*** **re0** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-
m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

To install the software on re1:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* re1** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

Reboot both Routing Engines.

For example:

```
user@switch> request system reboot both-routing-engines
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the `show version` command.

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

Installing the Software on QFX10008 and QFX10016 Switches

Because the switch has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

WARNING: If graceful Routing Engine switchover (GRES), nonstop bridging (NSB), or nonstop active routing (NSR) is enabled when you initiate a software installation, the

software does not install properly. Make sure you issue the CLI `delete chassis redundancy` command when prompted. If GRES is enabled, it will be removed with the `redundancy` command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the `[edit routing-options]` hierarchy level to disable it.

1. Log in to the master Routing Engine's console.

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

2. From the command line, enter configuration mode:

   ```
   user@switch> configure
   ```

3. Disable Routing Engine redundancy:

   ```
   user@switch# delete chassis redundancy
   ```

4. Disable nonstop-bridging:

   ```
   user@switch# delete protocols layer2-control nonstop-bridging
   ```

5. Save the configuration change on both Routing Engines:

   ```
   user@switch# commit synchronize
   ```

6. Exit the CLI configuration mode:

   ```
   user@switch# exit
   ```

   After the switch has been prepared, you first install the new Junos OS release on the backup Routing Engine, while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

   After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the software version on the other Routing Engine.

7. Log in to the console port on the other Routing Engine (currently the backup).

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

8. Install the new software package using the `request system software add` command:

   ```
   user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
   x86-64-23.2R1.n-secure-signed.tgz
   ```

   For more information about the `request system software add` command, see the CLI Explorer.

9. Reboot the switch to start the new software using the `request system reboot` command:

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

   NOTE: You must reboot the switch to load the new installation of Junos OS on the switch.

   To abort the installation, do not reboot your switch. Instead, finish the installation and then issue the `request system software delete` *<package-name>* command. This is your last chance to stop the installation.

   All the software is loaded when you reboot the switch. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

   While the software is being upgraded, the Routing Engine on which you are performing the installation is not sending traffic.

10. Log in and issue the `show version` command to verify the version of the software installed.

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

    Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the master Routing Engine software.

11. Log in to the master Routing Engine console port.

    For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

12. Transfer routing control to the backup Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the `request chassis routing-engine master` command, see the CLI Explorer.

13. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

```
user@switch> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Backup
    Election priority              Master (default)

Routing Engine status:
  Slot 1:
    Current state                  Master
    Election priority              Backup (default)
```

14. Install the new software package using the `request system software add` command:

```
user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
x86-64-23.2R1.n-secure-signed.tgz
```

For more information about the `request system software add` command, see the CLI Explorer.

15. Reboot the Routing Engine using the `request system reboot` command:

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

NOTE: You must reboot to load the new installation of Junos OS on the switch.

To abort the installation, do not reboot your system. Instead, finish the installation and then issue the `request system software delete jinstall` *<package-name>* command. This is your last chance to stop the installation.

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation does not send traffic.

16. Log in and issue the `show version` command to verify the version of the software installed.

17. Transfer routing control back to the master Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the `request chassis routing-engine master` command, see the CLI Explorer.

18. Verify that the master Routing Engine (slot 0) is indeed the master Routing Engine:

```
user@switch> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)

outing Engine status:
  Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
```

Performing a Unified ISSU

You can use unified ISSU to upgrade the software running on the switch with minimal traffic disruption during the upgrade.

NOTE: Unified ISSU is supported in Junos OS Release 13.2X51-D15 and later.

Perform the following tasks:

- "Preparing the Switch for Software Installation" on page 108
- "Upgrading the Software Using Unified ISSU" on page 108

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

- Ensure that nonstop active routing (NSR), nonstop bridging (NSB), and graceful Routing Engine switchover (GRES) are enabled. NSB and GRES enable NSB-supported Layer 2 protocols to synchronize protocol information between the master and backup Routing Engines.

  To verify that nonstop active routing is enabled:

  NOTE: If nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

  ```
  user@switch> show task replication
          Stateful Replication: Enabled
          RE mode: Master
  ```

  If nonstop active routing is not enabled (`Stateful Replication` is `Disabled`), see Configuring Nonstop Active Routing on Switches for information about how to enable it.

- Enable nonstop bridging (NSB). See Configuring Nonstop Bridging on EX Series Switches for information on how to enable it.

- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the `request system snapshot` command.

Upgrading the Software Using Unified ISSU

This procedure describes how to upgrade the software running on a standalone switch.

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in Installing Software Packages on QFX Series Devices.

2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.

3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.

4. Start the ISSU:

   - On the switch, enter:

     ```
     user@switch> request system software in-service-upgrade /var/tmp/package-name.tgz
     ```

     where *package-name*.tgz is, for example, jinstall-host-qfx-10-f-x86-64-20.4R1.n-secure-signed.tgz.

     NOTE: During the upgrade, you cannot access the Junos OS CLI.

     The switch displays status messages similar to the following messages as the upgrade executes:

     ```
     warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get lost!
     ISSU: Validating Image
     ISSU: Preparing Backup RE
     Prepare for ISSU
     ISSU: Backup RE Prepare Done
     Extracting jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz ...
     Install jinstall-host-qfx-5-f-x86-64-19.2R1.n-secure-signed.tgz completed
     Spawning the backup RE
     Spawn backup RE, index 0 successful
     GRES in progress
     GRES done in 0 seconds
     Waiting for backup RE switchover ready
     GRES operational
     Copying home directories
     Copying home directories successful
     Initiating Chassis In-Service-Upgrade
     Chassis ISSU Started
     ISSU: Preparing Daemons
     ISSU: Daemons Ready for ISSU
     ISSU: Starting Upgrade for FRUs
     ISSU: FPC Warm Booting
     ISSU: FPC Warm Booted
     ISSU: Preparing for Switchover
     ISSU: Ready for Switchover
     Checking In-Service-Upgrade status
       Item           Status                  Reason
       FPC 0          Online (ISSU)
     Send ISSU done to chassisd on backup RE
     ```

```
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff
```

NOTE: A unified ISSU might stop, instead of abort, if the FPC is at the warm boot stage. Also, any links that go down and up will not be detected during a warm boot of the Packet Forwarding Engine (PFE).

NOTE: If the unified ISSU process stops, you can look at the log files to diagnose the problem. The log files are located at `/var/log/vjunos-log.tgz`.

5. Log in after the reboot of the switch completes. To verify that the software has been upgraded, enter the following command:

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

6. Ensure that the resilient dual-root partitions feature operates correctly, by copying the new Junos OS image into the alternate root partitions of all of the switches:

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

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 6: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

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

Junos OS Release Notes for SRX Series

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for SRX Series devices.

To view features supported on the SRX platforms, view the Feature Explorer using the following links. To see which features are supported in Junos OS Release 23.2R2, click the Group by Release link. You can collapse and expand the list as needed.

- SRX300
- SRX320
- SRX340
- SRX345
- SRX380
- SRX550 HM
- SRX1500
- SRX4100
- SRX4200
- SRX4600
- SRX5400
- SRX5600
- SRX5800

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series.

Content Security

- **New fallback option for antivirus (SRX Series and vSRX)**—We introduce the `server-connection-err` statement at the `edit security utm default-configuration anti-virus fallback-options` hierarchy level. This new statement enables you to configure the fallback actions when the device to Sophos server connection has an error due to following reasons:

  - Sophos server configuration does not have an SSL initiation profile.
  - Server host is not resolved.
  - Outgoing interface IP is not available.
  - Server to device connection creation failed due to internal errors.

  We've also enhanced the `show security utm anti-virus statistics` output with the `Server connection error` counter.

  See fallback-options (Security Antivirus Sophos Engine).

Network Management and Monitoring

- **NETCONF `<copy-config>` operations support a `file://` URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The NETCONF `<copy-config>` operation supports using a `file://` URI when `<url>` is the target and specifies the absolute path of a local file.

  [See <copy-config>.]

VPNs

- **Enhancements to IKE configuration management for clearing IKE stats on secondary node (SRX Series)**—In Earlier Junos OS Releases, in a Chassis Cluster mode, the ike-config-Management (IKEMD) process did not respond to management requests on the secondary node. The command `clear security ike stats`, fails with the error message `error: IKE-Config-Management not responding to management requests` on the secondary node. Starting in Junos OS Release 22.4R3, the command runs successfully without the error on the secondary node.

- **Introduction of extensive option for IPsec security associations (MX Series, SRX Series and vSRX 3.0)**—We've introduced the `extensive` option for the `show security ipsec security-associations` command. Use this option to display IPsec security associations with all the tunnel events. Use the existing `detail` option to display upto ten events in reverse chronological order.

  See **show security ipsec security-associations**.

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for SRX Series devices.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Infrastructure

- First time when you add connection-limit command the existing active connections are not changed, only the new connection after this command will be taken into effect. PR1608715
- On SRX380, the autonegotiation status on the 1G and 10G ports might be incorrectly displayed as "Incomplete". This has no impact to traffic. PR1703002
- BCM5342X SOC port configurations, BCM53426 don't have QSGMII interface. Only the QSGMII port supports half-duplex mode. SRX340 and SRX345 have only SGMII interface, hence half-duplex is not supported. PR1716094

Open Issues

IN THIS SECTION

Learn about open issues in this release for SRX Series Firewall devices.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Authentication and Access Control

- On SRX Series Firewall on aruba-clearpass webapi configuration set system services webapi * authentication entries could be lost during ISSU or during Junos version upgrades to 23.1 from prior versions. Due to this issue any data plane traffic using the ClearPass Authentication entries will require reauthentication.PR1732210

Flow-Based and Packet-Based Processing

- For accelerated flows such as Express Path, the packet or byte counters in the session close log and show session output take into account only the values that accumulated while traversing the NP. PR1546430
- In NAT46 or NAT64 scenario, the IPv4 packet that incoming from interface has only family inet ,do the NAT4to6 and send out to an IPv6 interface then trigger the NDP learning or the IPv6 packet incoming from interface has only family inet6 to the NAT6to4 and then trigger ARP learning, this packet might get dropped in the Packet Forwarding Engine.PR1759202

- On SRX Series Firewall, in a chassis cluster setup configured in Active/Active mode, the fabric forward packet enters the flow module causing the flow processing process (flowd) to crash, impacting the traffic forwarding and failing the Services Processing Card (SPC).PR1761542

General Routing

- IPsec rekey fails when SRX Series Firewall is configured with KB based lifetime in remote access solution. PR1527384
- When non-root user tries to generate archive file for /var/log, it either fails or generates an archive with partial log files. This happens due to permission of files under /var/log/hostlogs/.PR1692516
- FIPS mode is not supported in this release for SRX Series Firewall devices.PR1697999
- Mount Command from shell mode is not supported for NFS in BSD12 based SRX300, SRX320, SRX340, SRX345, and SRX380 platforms. PR1701361
- On SRX Series Firewall, log streaming using FQDN requiring DNS name resolution might fail to re-query resulting in FQDN resolution to fail.PR1708116
- For case when input traffic is more and output traffic is expected equal to maximum capacity of egress interface, please set the shaping explicitly equal to interface maximum capacity if default shaping does not work. PR1712964
- On SRX Series Firewall, The delay will be observed while pinging to peer device due to high latency when VLAN tagged DHCP packets arrive at IRB interface.PR1714620
- In DNS response packets from the DNS server, the DNS flags do not have RA (Recursion Available) enabled. SRX Series Firewall discovers that this RA flag is disabled, and processes it as an error. The SRX Series Firewall then sends another DNS query to the second DNS server.PR1716171
- It is possible to set and commit the datapath-debug configuration on platforms SRX4100 and SRX4200 although datapath debugging is not supported on those platforms. Because of this unsupported configuration being accepted the Routing Engine load can go high and cause traffic outage. The workaround is to remove the datapath-debug configuration and perform a commit.PR1739559
- On SRX Series Firewall in cluster, the IP Monitoring fails to install route after the SRX Series Firewall cluster reboots.PR1780326

J-Web

- If session limit not configured in CLI, default value of session limit will be 7 or 1024.PR1788364
- On SRX Series Firewall, J-Web does not display address book entries properly after certain operations.PR1789466

Content Security

- On SRX Series Firewall with multiple security policies configured and different web-filtering profiles attached to them, policies don't work as per the action defined in them.PR1696642

VPNs

- First time when we add this command the existing active connections are not changed, only the new connection after this command will be taken into effect. PR1608715

Resolved Issues

Learn about the issues fixed in this release for SRX Series Firewall.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Content Security

- The utmd process might generate core files at commit when *.* or *.*.* is configured at url-pattern. PR1715260
- Outlook notification channel connection is not established. PR1725938
- When SSL proxy and Web filtering are enabled in the security policy, Youtube videos will keep on buffering and will not play. As a workaround, configure the `no-safe-search` option at the Web filtering profile. PR1755998

Application Layer Gateways (ALGs)

- Device stopped while processing H323 traffic in SRX Series Firewall and MX. PR1722877
- SIP ALG not working for SIP traffic with MIME header and traffic is dropped. PR1728638

Chassis Clustering

- Unsupported configuration for interface st0.16000-16385 is possible when using replace pattern on SRX Series Firewall. PR1731593
- In SRX Series Firewall MNHA cluster setup the RSI takes long time to generate. PR1736498
- BFD session fails to re-establish on SRX Series Firewall cluster mode. PR1737520
- SRX Series Firewall dropping GTP ChangeNotificationRequest messages due to Non-zero TID/TEID. PR1750988

Class of Service (CoS)

- The CoS scheduler map will not get attached to the sub-interface correctly when shaping-rate and scheduler-map are configured on it. PR1734013

Flow-Based and Packet-Based Processing

- The datapath-debug packet-dump feature is not capturing the transit traffic packets. PR1727027
- SRX5000 line of devices or SRX4600 is forwarding the traffic with previous MAC address, even though the ARP table is pointing to a new MAC address. PR1755181
- Buffer leak when PMI sends out packet on egress interface with MTU smaller than the packet length. PR1758208

General Routing

- On SRX4600, packet drop or a core file gets generated. PR1620773
- 8-Port Gigabit Ethernet SFP XPIM not passing traffic after software upgrade. PR1620982
- The DNS information is getting lost when IPCP flaps. PR1658968
- The fxp0 interface works under disable state on SRX300. PR1661816
- Unable to connect to domain controller on installing Microsoft KB update. PR1683420
- The user ID entries are not synced with secondary node. PR1701990

- Secondary node goes into disabled state after failover due to control link going down in a cluster. PR1703220
- Interface speed stays 100 Mbps when removing speed and duplex command separately. PR1715247
- J-flow sends wrong IP in sampling records when NAT is configured for traffic along with input sampling. PR1716707
- OAM not working with flexible-vlan-tagging. PR1719108
- Local route is not added in the secondary FIB on all Junos SRX Series Firewall and routes will be permanently stuck in KRT queue. PR1721032
- Nstraced process is running high on the primary node after the Junos upgrade. PR1727122
- Layer 2 channel error counter increases when unknown family packets received by interfaces. PR1729284
- When there is a power outage happens after the first upgrade, the reboot device gets stuck at volume booting. PR1729671
- The show system firmware shows available version as 0 after upgrading to BSD12 image. PR1729959
- The DNS cache gets wiped out due to the flowd process pause on all SRX Series Firewall after the upgrade. PR1732028
- The flowd-octeon.elf process generate core files in SRX380 cluster. PR1732378
- The nsd process stop impacting remote access VPN on SRX Series Firewall. PR1732746
- The intermittent core files are received when SMB protocol is enabled on AAMW policy and Packet Forwarding Engine memory is exhausted. PR1737442
- Junos OS installation using USB can fail on SRX4600. PR1737721
- Failover can be seen on SRX5000 line of devices with SPC2 cards while executing RSI. PR1738188
- The minor autorecovery information needs to be saved alarm is not displayed after zeroize. PR1738271
- Traffic drop caused by Packet Forwarding Engine memory leak on SRX Series Firewall. PR1738656
- Memory leak in PKID process. PR1739342
- Random physical interfaces doesn't come up after a reboot. PR1739520
- SRX4100 and SRX4200 accepts the datapath-debug configuration although it does not support it. PR1739559

- Processing a TWAMP packet and terminating the TWAMP session might generate core files in a corner case scenario. PR1739733
- The flowd process pause might be observed. PR1743107
- Commit panic reboot observed after implementing system processes watchdog timeout 180 on SRX Series Firewall. PR1744108
- Add FQDN-name counter in the show services user-identification identity-management status output. PR1745588
- SRX4600 misleading fan speed syslog output after removing or inserting one fan tray unit. PR1748971
- SRX Series Firewall will take time to come up in HA or device will go down in standalone setup. PR1749584
- SPC3 PIC stops. PR1749830
- Large TLS1.3 session tickets to an SRX SPC3 device result in srxpfe process pause. PR1752678
- The flowd process stops due to memory stress. PR1753540
- Users authenticated through captive portal experience a noticeable delay of atleast 2-to 5 minutes. PR1755593
- AAMW hyper scan goes to lock state during reload. PR1757794
- The set system license log-frequency time-interval command does not work. PR1766874
- ARP is not getting resolved. PR1768050

Intrusion Detection and Prevention (IDP)

- Multiple network issues are seen after the upgrade with lower IDP packet-log total-memory percentage. PR1741887

J-Web

- The process httpd stops on SRX Series Firewall. PR1732269
- Editing security policy configuration via J-web is enabling "Exclude Selected" unexpectedly. PR1735314
- Junos OS: EX and SRX Series: A PHP vulnerability in J-Web allows an unauthenticated to control important environment variables (CVE-2023-36845) PR1736942

- Certificate Management issues. PR1738316
- Cannot add custom defined security address-book under Security Policies Objects > Security Policies > Create > Source Zone > Select Sources. PR1748078
- Junos OS upgrade from J-Web returns "failed" in each step. PR1755072

Layer 2 Ethernet Services

- Delay in getting IP through DHCP cause traffic loss. PR1752804

Network Address Translation (NAT)

- The nsd process stops when ISSU is performed on the cluster. PR1724777

Platform and Infrastructure

- The message "kernel: %KERN-6: ARP UNICAST MODE 0; retrans_timer - 8" might be seen when commit command is run for configuration which is not related to ARP. PR1735686

Routing Policy and Firewall Filters

- Traffic impact is observed when the security policy is configured with a huge number of addresses and on addition and deletion of these policies. PR1725567

Routing Protocols

- BFD session for BGP remains down in a specific scenario. PR1738074
- Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute (CVE-2023-0026) PR1739919
- RPD scheduler slip is observed when the BGP session flaps and subsequent configuration changes for the same peer. PR1742416
- When BGP is configured in routing-instance of type virtual-router, default MPLS table is being created for that virtual-router, unexpectedly. PR1742513

User Interface and Configuration

- The mgd process might stopdue to stack overflow on high scale address configuration. PR1741413

VLAN Infrastructure

- On SRX Series Firewall working as Layer 2 mode, packet and byte counters in flow session result or traffic log were not correct for traffic uses UTM or ALG services. PR1787772

VPNs

- IPsec VPN does not come up in NAT-T scenario. PR1745174
- Error seen while clearing ike statistics in secondary node. PR1748531

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for SRX Series devices. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

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

For information about ISSU, see the Chassis Cluster User Guide for Security Devices.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 7: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

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

Junos OS Release Notes for vMX

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for vMX.

What's Changed

IN THIS SECTION

Learn about what changed in this release for vMX.

Network Management and Monitoring

- **NETCONF `<copy-config>` operations support a `file://` URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The NETCONF `<copy-config>` operation supports using a `file://` URI when `<url>` is the target and specifies the absolute path of a local file.

  [See <copy-config>.]

Known Limitations

There are no known limitations in hardware or software in this release for vMX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Open Issues

There are no known issues in hardware or software in this release for vMX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for vMX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- Total LSP count mismatch on path computation client after PCCD restart. PR1714158

Upgrade Instructions

You cannot upgrade Junos OS for the vMX router from earlier releases using the `request system software add` command.

You must deploy a new vMX instance using the downloaded software package.

Remember to prepare for upgrades with new license keys and/or deploying Agile License Manager.

Junos OS Release Notes for vRR

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for vRR.

What's Changed

There are no changes in behavior and syntax in this release for vRR.

Known Limitations

There are no known limitations in hardware or software in this release for vRR.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

To learn more about common BGP or routing known limitations in Junos OS 23.2R2, see "Known Limitations" on page 40 for MX Series routers.

Open Issues

There are no known issues in hardware or software in this release for vRR.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Resolved Issues

Learn about the issues fixed in this release for vRR.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Routing Protocols

- The DNS cache gets wiped out due to the flowd process stops on SRX Series Firewall after the upgrade. PR1732028
- Constant BGP peer flaps might generate core files. PR1732833
- Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute (CVE-2023-0026) PR1739919

Junos OS Release Notes for vSRX

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for vSRX.

What's Changed

IN THIS SECTION

Learn about what changed in this release for vSRX.

Content Security

- **New fallback option for antivirus (SRX Series and vSRX)**—We introduce the `server-connection-err` statement at the `edit security utm default-configuration anti-virus fallback-options` hierarchy level. This new statement enables you to configure the fallback actions when the device to Sophos server connection has an error due to following reasons:
  - Sophos server configuration does not have an SSL initiation profile.
  - Server host is not resolved.
  - Outgoing interface IP is not available.
  - Server to device connection creation failed due to internal errors.

  We've also enhanced the `show security utm anti-virus statistics` output with the `Server connection error` counter.

  See fallback-options (Security Antivirus Sophos Engine).

Network Management and Monitoring

- **NETCONF <copy-config> operations support a file:// URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The NETCONF <copy-config> operation supports using a file:// URI when <url> is the target and specifies the absolute path of a local file.

  [See <copy-config>.]

VPNs

- **Introduction of extensive option for IPsec security associations (MX Series, SRX Series and vSRX 3.0)**—We've introduced the extensive option for the show security ipsec security-associations command. Use this option to display IPsec security associations with all the tunnel events. Use the existing detail option to display upto ten events in reverse chronological order.

  See **show security ipsec security-associations**.

Known Limitations

There are no known limitations in hardware or software in this release for vSRX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Open Issues

IN THIS SECTION

Learn about open issues in this release for vSRX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Infrastructure

- On SRX Series Firewall, log streaming using FQDN requiring DNS name resolution may fail to re-query resulting in FQDN resolution to fail. PR1708116
- In DNS response packets from the DNS server, the DNS flags do not have Recursion Available (RA) enabled. SRX Series Firewall discovers that this RA flag is disabled, and processes it as an error. The SRX Series Firewall then sends another DNS query to the second DNS server. PR1716171

Resolved Issues

Learn about the issues fixed in this release for vSRX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Flow-Based and Packet-Based Processing

- On SRX Series Firewall, tunnel fails to come up when tunnel destination routing instance is configured. PR1693767
- The inet6 packet mode drops traffic significantly. PR1733819
- Virtual Routing Instance configured on ingress interface might drop the icmp traffic. PR1742739
- Buffer leak when PMI sends out packet on egress interface with MTU smaller than the packet length. PR1758208
- Multicast packets of specific size between 663 to 676 bytes getting dropped. PR1761891

General Routing

- The DNS cache gets wiped out due to the flowd process stops on all SRX Series Firewall after the upgrade. PR1732028
- Traffic drop caused by Packet Forwarding Engine memory leak on SRX Series Firewall. PR1738656
- Memory leak in PKID. PR1739342
- Add FQDN-name counter in the show services user-identification identity-management status output. PR1745588

J-Web

- Junos OS: SRX Series: A vulnerability in J-Web allows an unauthenticated attacker to upload arbitrary files (CVE-2023-36846) PR1735389
- Junos OS: EX and SRX Series: A PHP vulnerability in J-Web allows an unauthenticated to control important environment variables (CVE-2023-36845) PR1736942
- Certificate Management issues. PR1738316
- J-Web gets stuck with loading message 'Please wait, syncing data from device'. PR1756252

Layer 2 Ethernet Services

- Delay in getting IP through DHCP cause traffic loss. PR1752804

VPNs

- ARI routes are sometimes not added after tunnel establishment. PR1735358

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains information about how to upgrade Junos OS for vSRX using the CLI. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

You also can upgrade to Junos OS Release 23.2R1 for vSRX using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

Direct upgrade of vSRX from Junos OS 15.1X49 Releases to Junos OS Releases 17.4, 18.1, 18.2, 18.3,18.4, 19.1, 19.2 and 19.4 is supported.

The following limitations apply:

- Direct upgrade of vSRX from Junos OS 15.1X49 Releases to Junos OS Release 19.3 and higher is not supported. For upgrade between other combinations of Junos OS Releases in vSRX and vSRX 3.0, the general Junos OS upgrade policy applies.
- The file system mounted on /var usage must be below 14% of capacity.

  Check this using the following command:

```
show system storage | match " /var$" /dev/vtbd1s1f
 2.7G        82M       2.4G        3%  /var
```

  Using the `request system storage cleanup` command might help reach that percentage.
- The Junos OS upgrade image must be placed in the directory /var/host-mnt/var/tmp/. Use the `request system software add /var/host-mnt/var/tmp/<upgrade_image>`
- We recommend that you deploy a new vSRX virtual machine (VM) instead of performing a Junos OS upgrade. That also gives you the option to move from vSRX to the newer and more recommended vSRX 3.0.
- Ensure to back up valuable items such as configurations, license-keys, certificates, and other files that you would like to keep.

NOTE: For ESXi deployments, the firmware upgrade from Junos OS Release 15.1X49-Dxx to Junos OS releases 17.x, 18.x, or 19.x is not recommended if there are more than three network adapters on the 15.1X49-Dxx vSRX instance. If there are more than three network adapters and you want to upgrade, then we recommend that you either delete all the additional network adapters and add the network adapters after the upgrade or deploy a new vSRX instance on the targeted OS version.

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 21.1R1 for vSRX .tgz** file from the Juniper Networks website. Note the size of the software image.
2. Verify that you have enough free disk space on the vSRX instance to upload the new software image.

```
root@vsrx> show system storage
       Filesystem             Size       Used      Avail  Capacity   Mounted on
```

```
        /dev/vtbd0s1a           694M       433M       206M       68%  /
        devfs                   1.0K       1.0K         0B      100%  /dev
        /dev/md0                1.3G       1.3G         0B      100%  /junos
        /cf                     694M       433M       206M       68%  /junos/cf
        devfs                   1.0K       1.0K         0B      100%  /junos/dev/
        procfs                  4.0K       4.0K         0B      100%  /proc
        /dev/vtbd1s1e           302M        22K       278M        0%  /config
        /dev/vtbd1s1f           2.7G        69M       2.4G        3%  /var
        /dev/vtbd3s2             91M       782K        91M        1%  /var/host
        /dev/md1                302M       1.9M       276M        1%  /mfs
        /var/jail               2.7G        69M       2.4G        3%  /jail/var
        /var/jails/rest-api       2.7G        69M       2.4G      3%  /web-api/var
        /var/log                2.7G        69M       2.4G        3%  /jail/var/log
        devfs                   1.0K       1.0K         0B      100%  /jail/dev
        192.168.1.1:/var/tmp/corefiles       4.5G       125M       4.1G    3%  /var/crash/
corefiles
        192.168.1.1:/var/volatile       1.9G       4.0K       1.9G    0%  /var/log/host
        192.168.1.1:/var/log       4.5G       125M       4.1G     3%  /var/log/hostlogs
        192.168.1.1:/var/traffic-log       4.5G       125M       4.1G    3%  /var/traffic-log
        192.168.1.1:/var/local       4.5G       125M       4.1G    3%  /var/db/host
        192.168.1.1:/var/db/aamwd       4.5G       125M       4.1G    3%  /var/db/aamwd
        192.168.1.1:/var/db/secinteld       4.5G       125M       4.1G    3%  /var/db/secinteld
```

3. Optionally, free up more disk space, if needed, to upload the image.

```
root@vsrx> request system storage cleanup
        List of files to delete:
        Size Date       Name
        11B Sep 25 14:15 /var/jail/tmp/alarmd.ts
        259.7K Sep 25 14:11 /var/log/hostlogs/vjunos0.log.1.gz
        494B Sep 25 14:15 /var/log/interactive-commands.0.gz
        20.4K Sep 25 14:15 /var/log/messages.0.gz
        27B Sep 25 14:15 /var/log/wtmp.0.gz
        27B Sep 25 14:14 /var/log/wtmp.1.gz
        3027B Sep 25 14:13 /var/tmp/BSD.var.dist
        0B Sep 25 14:14 /var/tmp/LOCK_FILE
        666B Sep 25 14:14 /var/tmp/appidd_trace_debug
        0B Sep 25 14:14 /var/tmp/eedebug_bin_file
        34B Sep 25 14:14 /var/tmp/gksdchk.log
        46B Sep 25 14:14 /var/tmp/kmdchk.log
        57B Sep 25 14:14 /var/tmp/krt_rpf_filter.txt
        42B Sep 25 14:13 /var/tmp/pfe_debug_commands
```

```
        0B Sep 25 14:14 /var/tmp/pkg_cleanup.log.err
        30B Sep 25 14:14 /var/tmp/policy_status
        0B Sep 25 14:14 /var/tmp/rtsdb/if-rtsdb
        Delete these files ? [yes,no] (no) yes
<
output omitted>
```

NOTE: If this command does not free up enough disk space, see [SRX] Common and safe files to remove in order to increase available system storage for details on safe files you can manually remove from vSRX to free up disk space.

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 21.1R1 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz /var/crash/corefiles/
```

5. From operational mode, install the software upgrade package.

```
root@vsrx> request system software add /var/crash/corefiles/junos-vsrx-
x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 20.4 software.
WARNING:     It will save JUNOS configuration files, and SSH keys
WARNING:     (if configured), but erase all other files and information
WARNING:     stored on this machine.  It will attempt to preserve dumps
WARNING:     and log files, but this can not be guaranteed.  This is the
WARNING:     pre-installation stage and all the software is loaded when
WARNING:     you reboot the system.
Saving the config files ...
Pushing Junos image package to the host...
Installing /var/tmp/install-media-srx-mr-vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
```

```
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz
Setting up Junos host applications for installation ...
============================================
Host OS upgrade is FORCED
Current Host OS version: 3.0.4
New Host OS version: 3.0.4
Min host OS version required for applications: 0.2.4
============================================
Installing Host OS ...
upgrade_platform: --------------------
upgrade_platform: Parameters passed:
upgrade_platform: silent=0
upgrade_platform: package=/var/tmp/junos-srx-mr-vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-
linux.tgz
upgrade_platform: clean install=0
upgrade_platform: clean upgrade=0
upgrade_platform: Need reboot after staging=0
upgrade_platform: --------------------
upgrade_platform:
upgrade_platform: Checking input /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz is valid.
upgrade_platform: Backing up boot assets..
cp: omitting directory '.'
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
initrd.cpio.gz: OK
upgrade_platform: Checksum verified and OK...
/boot
upgrade_platform: Backup completed
upgrade_platform: Staging the upgrade package - /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz..
./
./bzImage-intel-x86-64.bin
./initramfs.cpio.gz
./upgrade_platform
./HOST_COMPAT_VERSION
./version.txt
./initrd.cpio.gz
./linux.checksum
./host-version
```

```
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
upgrade_platform: Checksum verified and OK...
upgrade_platform: Staging of /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz completed
upgrade_platform: System need *REBOOT* to complete the upgrade
upgrade_platform: Run upgrade_platform with option -r | --rollback to rollback the upgrade
Host OS upgrade staged. Reboot the system to complete installation!
WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software rollback'
WARNING:     command as soon as this operation completes.
NOTICE: 'pending' set will be activated at next reboot...
Rebooting. Please wait ...
shutdown: [pid 13050]
Shutdown NOW!
*** FINAL System shutdown message from root@ ***
System going down IMMEDIATELY
Shutdown NOW!
System shutdown time has arrived\x07\x07
```

If no errors occur, Junos OS reboots automatically to complete the upgrade process. You have successfully upgraded to Junos OS Release 21.1R1 for vSRX.

NOTE: Starting in Junos OS Release 17.4R1, upon completion of the vSRX image upgrade, the original image is removed by default as part of the upgrade process.

6. Log in and use the `show version` command to verify the upgrade.

```
--- JUNOS 20.4-2020-10-12.0_RELEASE_20.4_THROTTLE Kernel 64-bit
JNPR-11.0-20171012.170745_fbsd-
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ # cli
root> show version
Model: vsrx
Junos: 20.4-2020-10-12.0_RELEASE_20.4_THROTTLE
JUNOS OS Kernel 64-bit  [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
```

```
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]
JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_ssd-builder_release_174_throttle]
```

Validating the OVA Image

If you have downloaded a vSRX .ova image and need to validate it, see Validating the vSRX .ova File for VMware.

Note that only .ova (VMware platform) vSRX images can be validated. The .qcow2 vSRX images for use with KVM cannot be validated the same way. File checksums for all software images are, however, available on the download page.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 8: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

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

Licensing

In 2020, Juniper Networks introduced a new software licensing model. The Juniper Flex Program comprises a framework, a set of policies, and various tools that help unify and thereby simplify the multiple product-driven licensing and packaging approaches that Juniper Networks has developed over the past several years.

The major components of the framework are:

- A focus on customer segments (enterprise, service provider, and cloud) and use cases for Juniper Networks hardware and software products.
- The introduction of a common three-tiered model (standard, advanced, and premium) for all Juniper Networks software products.
- The introduction of subscription licenses and subscription portability for all Juniper Networks products, including Junos OS and Contrail.

For information about the list of supported products, see Juniper Flex Program.

Finding More Information

- **Feature Explorer**—Juniper Networks Feature Explorer helps you to explore software feature information to find the right software release and product for your network.

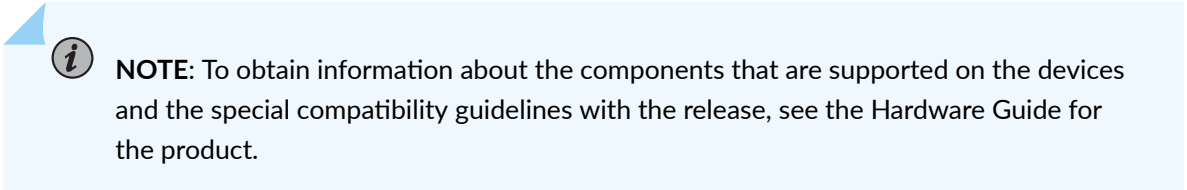
  https://apps.juniper.net/feature-explorer/

- **PR Search Tool**—Keep track of the latest and additional information about Junos OS open defects and issues resolved.

  https://prsearch.juniper.net/InfoCenter/index?page=prsearch

- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms.

  https://apps.juniper.net/hct/home



- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6.

  https://pathfinder.juniper.net/compliance/

Requesting Technical Support

IN THIS SECTION

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/

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

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

Creating a Service Request with JTAC

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

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

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

Revision History

30 October 2025—Revision 9, Junos OS Release 23.2R2.

24 September 2025—Revision 8, Junos OS Release 23.2R2.

14 August 2025—Revision 7, Junos OS Release 23.2R2.

27 March 2025—Revision 6, Junos OS Release 23.2R2.

19 September 2024—Revision 5, Junos OS Release 23.2R2.

8 August 2024—Revision 4, Junos OS Release 23.2R2.

30 May 2024—Revision 3, Junos OS Release 23.2R2.

25 April 2024—Revision 2, Junos OS Release 23.2R2.

29 March 2024—Revision 1, Junos OS Release 23.2R2.