Release Notes

Published
2025-08-14

Junos OS Release 22.4R3®

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion Enterprise, Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX. These release notes accompany Junos OS Release 22.4R3. They describe new and changed features, limitations, and known 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.

What's Changed

IN THIS SECTION

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

General Routing

- Two new alarms are added and can be seen with MPC11E when 400G-ZR optics are used. High Power Optics Too Warm: warning of the increase in chassis ambient temperature with no functional action taken on the optics Temperature too high for optics power on: New inserted optics when the chassis ambient temperature is elevated beyond the threshold will not be powered on and would need to be reinserted when the ambient temperature is within the acceptable range

- The packet rate and byte rate fields for LSP sensors on AFT (with the legacy path) have been renamed as jnx-packet-rate and jnx-byte-rate and is in parity with the UKERN behavior. Previously, these rate fields were named as packetRate and byteRate.

- 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.

- **Label-switched interface (LSI) delay during reboot (ACX Series)** — Rebooting ACX Series routers running Junos OS Evolved with a class-of-service routing-instance configuration might encounter errors due to a delay with the label-switched interface (LSI). LSI state information has been added to the output of the `show route instance` command to assist in the analysis of such errors.

  [See show route instance.]

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).]

- **Ability to restart restart daemonized applications**—Use the `request extension-service restart-daemonize-app` *`application-name`* command to restart a daemonized application running on a Junos device. Restarting the application can assist you with debugging and troubleshooting.

  [See request extension-service restart-daemonize-app.]

Network Management and Monitoring

- **Changes to the NETCONF server's <rpc-error> element when the operation="delete" operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the <rpc-error> response that the NETCONF server returns when the <edit-config> operation uses operation="delete" to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the <rpc-error> element includes the <error-tag>data-missing</error-tag> and <error-type>application</error-type> elements.

- **Changes to the RPC response for <validate> operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the rfc-compliant statement at the [edit system services netconf] hierarchy level, the NETCONF server emits only an <ok/> or <rpc-error> element in response to <validate> operations. In earlier releases, the RPC reply also includes the <commit-results> element.

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.

Known Limitations

IN THIS SECTION

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 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 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
- On WRL8 based VMHost platforms (i.e., ACX6360/PTX10001/MX150/NFX150/NFX250/NFX350), there is no log rotation for resild log and temperature sensor info is incorrectly written into resild log which could result in continuous logs in resild log file. The disk usage might keep increasing due to this issue. The disk usage could be eventually full which could cause system to hang and reboot. PR1480217
- Due to BRCM KBP issue route lookup may fail. Need to upgrade KBP to address this issue, Due to high risk KBP SDK upgrade planned for 21.1. PR1533513
- Service MIC does not work on ACX500 running Junos 20.4 or higher. PR1569103

- On all ACX Platforms, the hosts will not receive multicast traffic when snooping is configured in a EVPN-MPLS (Ethernet Virtual Private Network - Multiprotocol Label Switching) enabled broadcast domain.PR1613462
- A vulnerability in class-of-service (CoS) queue management in Juniper Networks Junos OS on the ACX2000 Series devices allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). PR1637615
- When TCP Main and TCP remaining attached together on IFD it is observed that Improper Scheduler MAP is getting configured on HQoS IFD while sched params modification and bind are performed on the same commit. This is a sequence issue from CoSD(RE) which is not guaranteed on the PFE side.PR1664785
- 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 ACX5000 Series. PR1665178
- The AE statistics might 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
- In a device with LACP configured and high rate of LLDP PDU packets of the order of around 400 PPS, LACP link state transitions were observed.PR1696723
- 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
- We might 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
- On ACX5448 platforms, the Tx laser is not turned off even if the port is disabled. This can be identified with the command `show interfaces diagnostics optics`. There is no service impact due to this issue. PR1735670
- On ACX1000 and ACX2000 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 ACX1000, ACX2000 and ACX3000 platforms, MPLS load-balancing on AE (Aggregated Ethernet) interfaces with more than one member link might not work as expected after upgrading Junos OS to 20.1R1 or later releases. PR1739480

- [TWM Clocking Solution] - chassis clock status should not move to **holdover** while switching between PTP path alone. PR1745604
- COS:ACX5448: Deactivate/Activate of fixed classifier does not work with wildcards configured. PR1754019
- On ACX5448 and ACX710 platforms, the Layer 3 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
- EXP bits are not modified according to default rewrite rule for bottom label on ACX5448. PR1757906
- ACX5448: cfm is stuck in start state between dut and service edge router. PR1760482

Infrastructure

- NTP time drift on the affected Junos releases. Earlier implementation of kvmclock with vDSO (virtual Dynamic Shared Object) which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate.PR1691036

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 might fail to come up. PR1633395
- ACX-5448: PPS values seen on interface even when it is in disabled state. PR1685344
- Interface queues display incorrect values of default reserved buffers. PR1689183
- 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
- Traffic drops seen after making COS configuration change on ACX710. PR1704589
- [interface] [acx_ifd] ACX7100-32C :: Can we unhide `set chassis cb` since we need customer to set CB temperature thresholds. PR1705035
- L2VPN traffic is dropped as the default MTU is less by 4 bytes. PR1707932
- The member interface will not be added to the AE bundle if the link-speed of the AE interface does not match that of the member. PR1713699
- The traffic through the AE member link will be dropped. PR1714111
- SFP-T cannot be recognized after detecting an I2C error on ACX5448. PR1715924
- SNMP MIB OID output showing wrong temperature value if device running under negative temperature. PR1717105
- 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
- The multicast packets could hit the CPU/RE on ACX5448 and ACX710 platforms. PR1722277
- Intermittent MAC move is observed in VPLS environment when ACX5448 or ACX710 is acting as a PE device. PR1722919
- Traffic is getting discarded in PFE when forwarding-table is changed. PR1723624
- Media MTU of ACX5448 will be 4 byte larger for transit packets. PR1724750

- [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
- Traffic drops on certain ACX platforms after it is upgraded. PR1731081
- 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
- 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
- EVPN routes does not work properly when resolution preserve-nexthop-hierarchy is 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 Layer 2 services. PR1756150
- Interface flaps leading to PFE crash due to FPC heap corruption. PR1764083
- Traffic convergence is longer than usual after the CoS rewrite. PR1770491

Interfaces and Chassis

- On Junos platforms the DCD will flap the IFLs which are part of EVPN routing-instance. PR1712800
- 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

Platform and Infrastructure

- TCP window scaling might be not applied to the first TCP packet sent to the client after the three-way handshake, leading to unnecessary segmentation. PR1761242

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 thirty six months after the first general availability date and customer support for an additional six more 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)	36 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

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

What's Changed

IN THIS SECTION

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

EVPN

- **Specify the UDP source port in a ping overlay or traceroute overlay operation**—In Junos OS releases prior to 22.4R1, you could not configure the `udp source port` in a ping overlay or traceroute overlay operation. You may now configure this value in an EVPN-VXLAN environment using `hash`. The configuration option `hash` will override any other hash options that may be used to determine the source port value.

General Routing

- Activation of SFP-10GBASE-T for 1G speed simultaneously with other 1G SFPs-If you want to use SFP-10GBASE-T at 1G speed, use a separate quad of ports. Do not mix with other 1G SFPs because SFP-10GBASE-T deactivates other ports with a different 1G SFP module.

Network Management and Monitoring

- **Changes to the NETCONF server's `<rpc-error>` element when the `operation="delete"` operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the `<rpc-error>` response that the NETCONF server returns when the `<edit-config>` operation uses `operation="delete"` to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the `<rpc-error>` element includes the `<error-tag>data-missing</error-tag>` and `<error-type>application</error-type>` elements.

- **Changes to the RPC response for `<validate>` operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server emits only an `<ok/>` or `<rpc-error>` element in response to `<validate>` operations. In earlier releases, the RPC reply also includes the `<commit-results>` element.

Platform and Infrastructure

- **The `ping host | display xml validate` command validates XML without error (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, and vMX)**—In the earlier releases of Junos OS and Junos OS Evolved release 22.4R2, the `ping host | display xml validate` command results in CRITICAL ERROR:

Root tag name mismatch. Expected 'ping-results', got 'run-command'. The command now validates the XML successfully without error.

[See ping.]

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.

EVPN

- EVPN-VXLAN: After Routing Engine switchover, you will see a momentary traffic loss with EVPN VXLAN on the EX4400 switches. PR1659315

General Routing

- On all Junos trinity-based platforms such as EX Series and MX Series, global port mirroring will not work for RSPAN scenario (port-mirror output as VLAN or bridge-domain). Port-mirror instance configuration `set forwarding-options port-mirroring instance` will work for RSPAN scenario. PR1668900
- MVRP on P-VLAN promiscuous port is not supported. If MVRP is configured on promiscuous port, then hosts connected to secondary VLAN ports will not be able to reach external world through promiscuous port carrying primary VLAN tags. PR1693345

- JUNOS_REG: EX4400 : input-vlan-tagged-frames are not in the expected range while verifying VLAN tagged Frames. PR1749391

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

Virtual Chassis

- EX4400 supports multiple uplink modules. Some supports Virtual Chassis port (VCP) conversion and some doesn't. Therefore, the recommended procedure is to convert VCP to NW port first and then make sure uplink module is made offline using `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.

EVPN

- After Routing Engine switchover, a momentary traffic loss may be observed with EVPN VxLAN on EX4400 switches. PR1659315

General Routing

- Runt, fragment and jabber counters are not incrementing on EX4300-MPs. PR1492605
- When launching a guest Virtual Machine (VM) to run a third party application on Junos OS release 15.1R1 and later, the guest VM might be shown as "UNAVAILABLE" even after successfully installing the third party application. This is due to duplicated device ID assigned to different disks. PR1529596
- When launching a guest virtual machine to run a third party application on the Junos OS 15.1R1 and above, the guest virtual machine might be shown as "UNAVAILABLE" even after successfully installing the third party application. This is due to duplicated device ID assigned to different disks. PR1529596
- Pause frame counters do not increment when pause frames are sent on the EX2300, EX3400, EX4300-48MP, and EX4300 line of switches. PR1580560
- In an interoperable scenario, when using 1G SFP optic on PIC-2, you must disable auto-negotiation on the peer. PR1657766
- On the EX4600 device with SFP-LX10/SFP-SX, after a power cycle or software reboot, all ports are initialized and links are up when you enable auto-negotiation. Few ports are up and traffic flows whereas few ports are up but no traffic flow through them.PR1672583
- If MVRP is enabled on an MSTP enabled interface, the interface will be made part of all the existing instances on the switch. If there are two interfaces between R1 and R2 as below: R1(et-0/0/1 and et-0/0/2)======(et-0/0/1 and et-0/0/2)R2. And one interface is MVRP enabled (say et-0/0/1), and et-0/0/2 is not MVRP enabled. By configuration et-0/0/1 is part of MSTI-1 and et-0/0/2 is part of MSTI-2. MSTI-1 is running on vlan-100 and MSTI-2 is running on Vlan-200. R2 in this case, is advertising only vlan-100. The MVRP enabled interface will become part of all the MSTIs (MSTI-1 and MSTI-2 both) configured on the device and it will take part in the FSM of all the MSTIs. Although et-0/0/1 is not member interface of vlan-200 (correspnding to MSTI-2). This potentially can cause a

problem where et-0/0/1 although not a vlan-200 member, will go into FWD state and et-0/0/2, genuine member of vlan-200 goes into BLK state for MSTI-2. When traffic is received in vlan-200 it will be sent out of et-0/0/1, an it will be dropped.PR1686596

- When you enable port beacon LED for the port, `show chassis led` statement output shows incorrect port LED status for the interfaces as lit up instead of off. PR1697678
- EX4600 with redundant trunk group (RTG) configured, after VCP port between members of EX4600 disconnect and connect again. MAC address entry created in RTG cannot ageout. PR1707878
- When high number of MACsec sessions present (more than 200) and traffic is passed over these interface, some of the MACsec session flap and there is traffic drop.PR1709431
- 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 rare case and would impact traffic as due to dcpfe failure the Packet Forwarding Engine restarts, so the interfaces will flap.PR1711860
- On EX4650 and QFX5120-Y, the 10G interfaces are not coming up simultaneously when different Small Form-factor Pluggable(SFPs - 10G and 1G) are plugged in within the same 4 port group. Normally 10G interface by itself will be up when set to 1G if no other SFP is plugged in.PR1714833
- This is a Broadcom limitation and Day 1 issue affecting broadcom chipsets such as EX4650's, QFX5ks, 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
- `request system reboot usb` doesn't seems to be supported in EX4300-48MP(tvp based model) Generally if want to upgrade image from USB in EX4300-48MP. Follow the below steps:
  - reboot the device
  - go to BIOS Manager
  - select USB to boot and upgrade image

  PR1734925
- On EX4400, request system halt/power off CLI doesn't turn off rear FAN LEDs.PR1737500
- On EX4400, a "BCM Error: API bcm_plp_mode_config_set" error msg may be seen in the syslog when converting a VCP to network port. There is no functionality impact.PR1738410
- In case of role swap along with fpc slot change between master and linecard, the older ifds are retained on master. PR1740024
- On EX2300, on VCP enable and disable, "optic_set_activity_led" error messages may be seen. There is no functionality impact for these error messagesPR1740064

- EX4400: With pre existing configuration of 1g for the uplink interfaces, the 1G uplink ports might not come up on 4x10G module insertion event.PR1741724
- When system comes up with BULK L2 configuration, a subsequent CONFIG delete in a way that L2ALD is still not finished processing the configuration create, could lead to a race condition where FLOOD ROUTE DEL event can cause l2ald crash. PR1742613
- Disable the vme interfaces or have the default route added properly from the shell script for the connectivity with the ztp server to work.PR1743222
- On EX2300 when zeroise is /var/db/leases gets deleted and due to this dhcp-client ip-address is not saved. PR1743467
- On EX4100, VC formation will not happen automatically after zeroize each device will function as Standalone. PR1744190
- On 1G port if tx rate is applied with 4m(Q0) + 996m (Q1). Configuration fails in COSD with the following log and not get pushed to PFE. COSD_TX_QUEUE_RATES_TOO_HIGH: cos_validate_scheduler_shaper_conflict:820 : Unable to apply scheduler map CPE-Transmit-VPN1G-normal-only to interface ge-x/x/x: sum of scheduler transmission rates exceeds interface shaping or transmission rate. PR1759821
- 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.PR1742565
- EX4400 could be stuck during boot, when one end of the twisted pair cable is connected to the primary console port and the other end is left unconnected/dangling.PR1754548
- EX-hardening: EX4400: set chassis config-button no-clear is not working. PR1758042
- On all Junos OS platforms, a warning message is seen when installing the license key where features don't support the product.PR1766515
- EX2300 VC: 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 rebootPR1775479
- When there are a large number of aggregated Ethernet 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

- GRES do not support the configuration of a private route, such as fxp0, when imported into a non-default instance or logical system. As work around, see KB26616resolution rib policy is required to apply. PR1754351

Layer 2 Ethernet Services

- Name-server resolution failure may be seen intermittently after zeroize or loading factory default config resulting in MIST on-boarding failure. Workaround is to restart dhcp-service. PR1747800

Layer 2 Features

- The memory might leak because of the eswd daemon on the EX Series platforms. A message like the following is displayed in the system log: eswd[1330]: JTASK_OS_MEMHIGH: Using 212353 KB of memory, 158 percent of available /kernel: KERNEL_MEMORY_CRITICAL: System low on free memory, notifying init (#2). /kernel: Process (1254,eswd) has exceeded 85% of RLIMIT_DATA: used 114700 KB Max 131072 KB. PR1262563

MPLS

- On Junos OS 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

- In mixed mode virtual Chassis (vc) when the 10G DAC is used as a Virtual Chassis Port (VCP) between Junos QFX5100 and EX4300 VC, the 10G DAC VCP will not come up after rebooting EX4300.PR1665250
- On EX4300 platform, if you configure `encapsulation ethernet-bridge` statement, the interface is getting programmed as trunk instead of access in VLAN membership. This leads to untagged traffic drop. PR1665785

- On EX4300-24T, EX4300-48P, EX4300-VC, EX430024P, EX430032F and EX430048T platforms, when a VSTP (VLAN Spanning Tree Protocol) BPDU (Bridge Protocol Data Unit) arrives with a VLAN ID that is not configured in the switch, but that matches with an HW Token of any other configured VLAN, the VLAN ID of the BPDU will be changed to the VLAN ID corresponding to the matched HW Token and flooded. This disrupts STP convergence on the configured VLAN because some ports can incorrectly go into blocking state. PR1673000
- 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 OS 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-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 EX4300MP-EX4300 mixed VC setup, "show system software sets" command shows 'Pending set' software version even after rebooting.PR1738406
- On EX4300 VC setup, "qsfp_tk_read_mem_page: Rear QSFP+ PIC failed to select addr 127 err 1000" messages may be seen intermittently. There is no functionality impact for these error messagesPR1747126
- After an upgrade, the SFP modules are not detected in case of EX4300 platforms and the ports remain down impacting traffic.PR1747374
- On EX4300, "Error requesting CMTFPC SET INTEGER" and "Error requesting SET BOOLEAN" logs may be seen after device boot up. There is no functional impact for the error messagesPR1749289
- On all EX4300 platforms, traffic is sent on an AE interface and sent to the removed child interface from AE (Aggregated Ethernet) where the traffic is lost.PR1749406
- On EX Series 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

Routing Protocols

- 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 configuration 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 greater than 90 percent. 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

Virtual Chassis

- On Junos EX4600 Virtual Chassis (VC), the primary Routing Engine reboot and all-members reboot lead to the Packet Forwarding Engine manager hogging logs when SFP-T pluggable is installed in. The Packet Forwarding Engine manager hogging logs has no functionality impact. PR1685067
- On EX4600-VC, when you execute the `request system reboot all members` statement, post-reboot one of the Virtual Chassis member or Flexible PIC Concentrator (FPC) might disconnect and join the Virtual Chassis back due to Packet Forwarding Engine restart. Traffic loss is seen when FPC disconnects. 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.

Forwarding and Sampling

- The Firewall filter with syslog action will not work when applied on the ingress of a loopback interface. PR1714988

General Routing

- EX4100 and EX4100-F virtual chassis: non-existing PIC ports are seen in Junos Telemetry queries. PR1681673
- fxpc daemon core file is observed on the Junos OS EX4400 platforms in a virtual chassis setup with HGoE mode. PR1682960
- With the logout-on-disconnect configuration, the prompt for setting the root authentication password on the console will not appear PR1686364
- 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
- Traffic loss is observed in IP fabric when there is a change in the underlay network. PR1688323
- Transceiver not detected after it's unplugged and plugged in again. PR1696444
- Traffic loss can be seen while switching between primary and fallback sessions in MACsec setup. PR1698687
- Traffic impact is observed when OSPF adjacency gets stuck in exstart or exchange state. PR1699216

- DHCP offer requests are dropped while routed towards different VRFs of transit router. PR1700203
- EX4400: pps counter does not show correct values for jubmo frames. PR1700309
- The operational state of the interface is displayed as not down even after disabling it, though the interface status is down. PR1701444
- Traffic blackhole in the event of a link failure (Rx LOS) for 1GE-SX/LX optics. PR1705461
- With MAC limit and persistent MAC learning configuration l2ald process will crash when MAC is learned through remote peers. PR1706364
- In a VC scenario, sometimes the alarms raised on the line-card or backup-RE may not show on the master Routing Engine. PR1707798
- License expire error will be observed after upgrade. PR1708794
- On EX4400, `show chassis environment power-supply-unit` displays only master member's details. PR1709483
- Certain EX Series platforms with option-18 configured may hinder the DHCPv6 process. PR1710360
- The link does not come up after PIC offline and online operation. PR1710793
- When a 100G transceiver is used as a VC port or network port, the VC port or network port will either not come up or come up as 40G. PR1711407
- DHCPv6 packets could not be forwarded if it contains the trailer or extra bytes out of the IP stack. PR1711525
- MACsec dynamic CAK not working due to interoperability issue. PR1711561
- 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
- The multiple supplicant scenarios for dot1x do not work with MAC based tagging in the case of group-based policies. PR1713982
- On EX4650, jnxOperatingDescr.1.1.0.0 is populated with blank. PR1714056
- EX4400 link/activity LED is not lit when it transits to the factory default configuration by pressing the factory reset/mode button. PR1714116
- On EX4400 and EX4400-24X platforms, BIOS upgrade is not getting successful via CLI. PR1715258
- MACsec may not work after reboot on broadcom pltforms with macsec hard enforcement license enabled(EX4000 and QF5000). PR1715308

- Traffic loss is seen on RTG bound interface. PR1715518
- The interface phy of PIC 0 comes up causing traffic loss while the device boots/reboots. PR1715680
- After the device reboots with lpm(longest prefix match) profile configured, the default route entry is getting created on IPv4 and IPv6 (pfe hw lpm) due to gRIBI routing instance and same route is removed after the interface flap. PR1715907
- EX4100MP (PSE) does not allocate a power value requested in LLDP by the PD. PR1716261
- The mac-move-limit (MMAS) flag is not getting reset after the interface recovers due to the l2-learning restart. PR1716270
- The link remains down on connecting the transceiver 10GBASE-T with the serial number starting with "2P1". PR1716703
- IGMP/MLD queries might drop if received on a port on the backup Virtual Chassis member when IGMP/MLD snooping is enabled. PR1716902
- DHCP services are impacted as DHCP binding will not work as expected. PR1718286
- The fxpc daemon crashes on Junos OS EX4400 platforms in a virtual chassis setup with HGoE mode. PR1718316
- Alarm "PEM is not supported/powered" might be seen after removing the power cable. PR1718825
- RSTP default configuration is missing when zeroize is performed. PR1719509
- Continuous messages indicating duplicate IP address L2ALM_DUPLICATE_IP_ADDR will be seen in MCLAG and VRRP scenario. PR1719868
- Port will be down when "no-auto-negotiation" is configured on EX4400-48F platform. PR1720074
- EX4400 shows incorrect interface et-0/0/0. PR1720257
- On EX4300-48MP I/O accesses to disk will fail. PR1720335
- In a rare case FPC crashes and reboots generating a core. PR1720591
- Interface with QSFP+-40G-CU50CM will be down. PR1720884
- On EX2300MP, error messages are observed during reboot/image upgrade. PR1721433
- Invalid "Power Class" value will be observed. PR1722674
- EX4400: Flow control shows as disabled at Packet Forwarding Engine, even after enabling it. PR1724188

- Traffic loss occurs with vlan tagging and/or vlan normalisation in a specific design (using a looped cable). PR1724675
- On certain Junos EX Series and QFX Series platforms the static ARP entries for DHCP-security are not present. PR1724933
- 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 seen on all Junos OS 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
- EAP dot1x authentication stuck in connecting state. PR1728538
- EX4400 VC: During upgrade/reboot , fxpc core files may be seen in a rare race condition. PR1728725
- Traffic loss will occur because of the CRC errors with QSFP+-40G-ACU10M plugged. PR1729067
- 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 is getting forwarded. PR1730076
- On EX4400, PIC2 details may not be not displayed for `show snmp mib walk entPhysicalVendorType` output. PR1731146
- Traffic for VLAN-id 2 drops in Ethernet-CCC L2 circuit on EX4650 platforms. PR1731291
- EX4400: Some log messages might flood 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

- Configuring CFM on ae interfaces on EX series virtual chassis will generate ppmd core files. 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
- EX4400: When SFPP-10G-T optics insterted in EX4400, IFD doesnt get created. PR1733920
- EX4300-48MP: Device did not come up with USB image when "request system reboot usb" is 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
- Junos OS: EX Series: A PHP vulnerability in J-Web allows an unauthenticated attacker to control important environment variables (CVE-2023-36844) PR1736937
- On EX4400, request system halt/power-off doesn't turn off FAN LED's. PR1737500
- Virtual Chassis 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
- 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 Series 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
- Both mge and ge interfaces are getting created for all ports during master member-id and role swap with Linecard. PR1740024

- On EX4400-48F, After phc commit in VC, default storm control config has extra xe port configuration 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
- Traffic drop will be observed after extended-vni-list configuration change with EVPN-VXLAN scenario. PR1742763
- 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, VC formation will not happen automatically after zeroize. PR1744190
- Enhancement of PoE Controller Firmware upgrade procedure. PR1744343
- Enhancement of PoE controller firmware files into Junos OS. PR1745088
- LLDP will not work on HGoE VC mode with 40G VCP connections. PR1747095
- PoE ports stop working after the reboot. PR1747128
- 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
- QFX: VC(virtual chassis) doesn't get formed when using 100G for vc port. PR1754838
- [EX4400/EX4100] A tranceiver fails to get detected on uplink module after 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
- EX4400:PSM is not detected in "show chassis hardware" until AC feed is connected to it. PR1759351
- The fxpc process might crash and cause traffic loss when adding and deleting irb configuration PR1760229
- LLDP neighborship will not be formed on all Junos devices PR1763053
- LLDP neighborship is not forming in non-master members PR1764085

Interfaces and Chassis

- DCD crash can be seen sometimes while pushing config using API. PR1742124

J-Web

- PHP vulnerability in J-Web allows an unauthenticated to control important environment variables (CVE-2023-36845). 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
- Dhcp security bindings may not happen when DHCP security is enabled on multiple vlans along with dhcp stateless relay. PR1731784
- Address allocation for DHCP client will fail if 'force-discover' configuration is enabled on client. PR1742696
- Name-server resolution failure may be seen intermittently after zeroize or loading factory default config resulting in MIST on-boarding failure. PR1747800

Platform and Infrastructure

- The vmcore crash observed in low memory conditions. PR1694463
- Traffic drop would be observed while restarting the chassis-control. PR1724563

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 (CVE-2023-0026). PR1739919
- Memory leak observed when reconfiguring the flow routes. PR1742147

Subscriber Access Management

- Intermittent authd crash will be seen on Junos platforms in a DHCP subscriber scenario. PR1697447

User Interface and Configuration

- After device reboot BGP sessions are not coming up 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 thirty six months after the first general availability date and customer support for an additional six more 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)	36 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

IN THIS SECTION

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.

Routing Protocols

Constant BGP peer flaps generate core rpd. PR1732833

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 thirty six months after the first general availability date and customer support for an additional six more 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)	36 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 Junos Fusion for Enterprise

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for Junos fusion for enterprise.

What's Changed

There are no changes in behavior and syntax in this release for Junos Fusion for enterprise.

Known Limitations

There are no known limitations in hardware or software in this release for Junos fusion for enterprise.

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 Junos Fusion for enterprise.

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 Junos Fusion for enterprise.

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

Junos Fusion Satellite Software

- The Junos Fusion Satellite device will be stuck in the SyncWait state. PR1682680

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the procedure to upgrade or downgrade Junos OS and satellite software for a Junos fusion for enterprise. Upgrading or downgrading Junos OS and satellite software might take several hours, depending on the size and configuration of the Junos fusion for enterprise topology.

Basic Procedure for Upgrading Junos OS on an Aggregation Device

When upgrading or downgrading Junos OS for an aggregation device, always use the `junos-install` 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 `junos-install` package and details of the installation process, see the Installation and Upgrade Guide.

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. See the Junos OS Administration Library.

To download and install Junos OS:

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:

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

2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

3. Select **By Technology > Junos Platform > Junos fusion** to find the software that you want to download.

4. Select the release number (the number of the software version that you want to download) from the Version drop-down list on the right of the page.

5. Select the **Software** tab.

6. Select the software package for the release.

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 `junos-install` package on the aggregation 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 commands, where *n* is the spin number.

```
user@host> request system software add validate reboot source/package-name.n.tgz
```

All other customers, use the following commands, where *n* is the spin number.

```
user@host> request system software add validate reboot source/package-name.n-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*** (available only for Canada and U.S. version)

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

Adding the `reboot` command reboots 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.

Upgrading an Aggregation Device with Redundant Routing Engines

If the aggregation device has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to minimize disrupting network operations as follows:

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*.

Preparing the Switch for Satellite Device Conversion

There are multiple methods to upgrade or downgrade satellite software in your Junos fusion for enterprise. See Configuring or Expanding a Junos fusion for enterprise.

For satellite device hardware and software requirements, see Understanding Junos fusion for enterprise Software and Hardware Requirements.

Use the following command to install Junos OS on a switch before converting it into a satellite device:

```
user@host> request system software add validate reboot source/package-name
```

NOTE: The following conditions must be met before a Junos switch that is running Junos OS Release 14.1X53-D43 can be converted to a satellite device when the action is initiated from the aggregation device:

- The switch running Junos OS can be converted only to SNOS 3.1 and later.
- Either the switch must be set to factory-default configuration by using the `request system zeroize` command, or the following command must be included in the configuration: `set chassis auto-satellite-conversion`.

When the interim installation has completed and the switch is running a version of Junos OS that is compatible with satellite device conversion, perform the following steps:

1. Log in to the device using the console port.

2. Clear the device:

```
[edit]
user@satellite-device# request system zeroize
```

NOTE: The device reboots to complete the procedure for resetting the device.

If you are not logged in to the device using the console port connection, your connection to the device is lost after you enter the **request system zeroize** command.

If you lose connection to the device, log in using the console port.

3. (EX4300 switches only) After the reboot is complete, convert the built-in 40-Gbps QSFP+ interfaces from Virtual Chassis ports (VCPs) into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port port-number
```

For example, to convert all four built-in 40-Gbps QSFP+ interfaces on an EX4300-24P switch into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 0
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 1
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 2
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 3
```

This step is required for the 40-Gbps QSFP+ interfaces that will be used as uplink interfaces in a Junos fusion topology. Built-in 40-Gbps QSFP+ interfaces on EX4300 switches are configured into VCPs by default, and the default settings are restored after the device is reset.

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, or preconfiguration. See Configuring or Expanding a Junos fusion for enterprise for detailed configuration steps for each method.

Converting a Satellite Device to a Standalone Switch

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove it from the Junos fusion topology. For more information, see Converting a Satellite Device to a Standalone Device.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

- 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 thirty six months after the first general availability date and customer support for an additional six more months.

For both 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
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

For more information about 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.

Downgrading Junos OS

Junos fusion for enterprise is first supported in Junos OS Release 16.1, although you can downgrade a standalone EX9200 switch to earlier Junos OS releases.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

To downgrade a Junos fusion for enterprise, follow the procedure for upgrading, but replace the `junos-install` package with one that corresponds to the appropriate release.

Junos OS Release Notes for Junos Fusion for Provider Edge

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for Junos Fusion for Provider Edge.

What's Changed

There are no changes in behavior and syntax in this release for Junos Fusion for provider edge.

Known Limitations

There are no known limitations in hardware or software in this release for Junos fusion for provider edge.

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 Junos Fusion for provider edge.

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

Junos Fusion Provider Edge

- On all Junos Fusion platforms, SDPD (Satellite Discovery and Provisioning Daemon) crash will be observed on the aggregation device (AD) while sending discovery packets for satellite device(SD) provision. Satellite provisioning will not be completed due to this issue and the SD cannot be managed from the AD. PR1624219

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for Junos Fusion for provider edge.

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

Junos Fusion Provider Edge

- The SDPD crash can be seen in Junos Fusion environment. PR1679794

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 Junos fusion for provider edge. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

Basic Procedure for Upgrading an Aggregation Device

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.

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. See the Installation and Upgrade Guide.

The download and installation process for Junos OS Release 22.4R2 is different from that for earlier Junos OS releases.

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:

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

2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

3. Select **By Technology > Junos Platform > Junos fusion** to find the software that you want to download.

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 page.

5. Select the **Software** tab.

6. Select the software package for the release.

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 aggregation 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 commands.

- For 64-bit software:

  NOTE: We recommend that you use 64-bit Junos OS software when implementing Junos fusion for provider edge.

  ```
  user@host> request system software add validate reboot source/jinstall64-22.4R2.SPIN-domestic-signed.tgz
  ```

- For 32-bit software:

  ```
  user@host> request system software add validate reboot source/jinstall-22.4R2.SPIN-domestic-signed.tgz
  ```

All other customers, use the following commands.

- For 64-bit software:

  NOTE: We recommend that you use 64-bit Junos OS software when implementing Junos fusion for provider edge.

  ```
  user@host> request system software add validate reboot source/jinstall64-22.4R2.SPIN-export-signed.tgz
  ```

- For 32-bit software:

  ```
  user@host> request system software add validate reboot source/jinstall-22.4R2.SPIN-export-signed.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*** (available only for the Canada and U.S. version)

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

Adding the `reboot` command reboots 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: After you install a Junos OS Release 22.4R2 `jinstall` package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the `jinstall` package that corresponds to the previously installed software.

Upgrading an Aggregation Device with Redundant Routing Engines

If the aggregation device has two Routing Engines, perform a Junos OS installation on each Routing Engine separately as follows to minimize disrupting network operations:

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*.

Preparing the Switch for Satellite Device Conversion

Satellite devices in a Junos fusion topology use a satellite software package that is different from the standard Junos OS software package. Before you can install the satellite software package on a satellite device, you first need to upgrade the target satellite device to an interim Junos OS software version that can be converted to satellite software. For satellite device hardware and software requirements, see Understanding Junos fusion Software and Hardware Requirements

NOTE: The following conditions must be met before a standalone switch that is running Junos OS Release 14.1X53-D43 can be converted to a satellite device when the action is initiated from the aggregation device:

- The switch can be converted to only SNOS 3.1 and later.
- Either the switch must be set to factory-default configuration by using the `request system zeroize` command, or the following command must be included in the configuration: `set chassis auto-satellite-conversion`.

Customers with EX4300 switches, use the following command:

```
user@host> request system software add validate reboot source/jinstall-ex-4300-14.1X53-D43.3-domestic-signed.tgz
```

Customers with QFX5100 switches, use the following command:

```
user@host> request system software add reboot source/jinstall-qfx-5-14.1X53-D43.3-domestic-signed.tgz
```

When the interim installation has completed and the switch is running a version of Junos and OS on one line that is compatible with satellite device conversion, perform the following steps:

1. Log in to the device by using the console port.
2. Clear the device:

```
[edit]
user@satellite-device# request system zeroize
```

NOTE: The device reboots to complete the procedure for resetting the device.

If you are not logged in to the device by using the console port connection, your connection to the device is lost after you enter the **request system zeroize** command.

If you lose your connection to the device, log in using the console port.

3. (EX4300 switches only) After the reboot is complete, convert the built-in 40-Gbps QSFP+ interfaces from Virtual Chassis ports (VCPs) into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port port-number
```

For example, to convert all four built-in 40-Gbps QSFP+ interfaces on an EX4300-24P switch into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 0
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 1
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 2
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 3
```

This step is required for the 40-Gbps QSFP+ interfaces that will be used as uplink interfaces in a Junos fusion topology. Built-in 40-Gbps QSFP+ interfaces on EX4300 switches are configured into VCPs by default, and the default settings are restored after the device is reset.

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, and preconfiguration. See Configuring Junos fusion for provider edge for detailed configuration steps for each method.

Converting a Satellite Device to a Standalone Device

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove the satellite device from the Junos fusion topology.

NOTE: If the satellite device is a QFX5100 switch, you need to install a PXE version of Junos OS. The PXE version of Junos OS is software that includes *pxe* in the Junos OS package name when it is downloaded from the Software Center—for example, the PXE image for Junos OS Release 14.1X53-D43 is named install-media-pxe-qfx-5-14.1X53-

D43.3-signed.tgz . If the satellite device is an EX4300 switch, you install a standard jinstall-ex-4300 version of Junos OS.

The following steps explain how to download software, remove the satellite device from Junos fusion, and install the Junos OS software image on the satellite device so that the device can operate as a standalone device.

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

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

2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

3. Select **By Technology > Junos Platform > Junos fusion** from the drop-down list and select the switch platform series and model for your satellite device.

4. Select the Junos OS Release 14.1X53-D30 software image for your platform.

5. Review and accept the End User License Agreement.

6. Download the software to a local host.

7. Copy the software to the routing platform or to your internal software distribution site.

8. Remove the satellite device from the automatic satellite conversion configuration.

   If automatic satellite conversion is enabled for the satellite device's member number, remove the member number from the automatic satellite conversion configuration. The satellite device's member number is the same as the FPC slot ID.

   ```
   [edit]
   user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
   satellite member-number
   ```

   For example, to remove member number 101 from Junos fusion:

   ```
   [edit]
   user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
   satellite 101
   ```

   You can check the automatic satellite conversion configuration by entering the `show` command at the `[edit chassis satellite-management auto-satellite-conversion]` hierarchy level.

9. Commit the configuration.

   To commit the configuration to both Routing Engines:

   ```
   [edit]
   user@aggregation-device# commit synchronize
   ```

   Otherwise, commit the configuration to a single Routing Engine:

   ```
   [edit]
   user@aggregation-device# commit
   ```

10. Install the Junos OS software on the satellite device to convert the device to a standalone device.

    ```
    [edit]
    user@aggregation-device> request chassis satellite install URL-to-software-package fpc-slot
    member-number
    ```

    For example, to install a PXE software package stored in the **/var/tmp** directory on the aggregation device onto a QFX5100 switch acting as the satellite device using FPC slot 101:

    ```
    [edit]
    user@aggregation-device> request chassis satellite install /var/tmp/install-media-pxe-
    qfx-5-14.1X53-D43.3-signed.tgz fpc-slot 101
    ```

    For example, to install a software package stored in the **var/tmp** directory on the aggregation device onto an EX4300 switch acting as the satellite device using FPC slot 101:

    ```
    [edit]
    user@aggregation-device> request chassis satellite install /var/tmp/jinstall-
    ex-4300-14.1X53-D30.3-domestic-signed.tgz fpc-slot 101
    ```

    The satellite device stops participating in the Junos fusion topology after the software installation starts. The software upgrade starts after this command is entered.

11. Wait for the reboot that accompanies the software installation to complete.

12. When you are prompted to log back into your device, uncable the device from the Junos fusion topology. See Removing a Transceiver from a QFX Series Device or Remove a Transceiver, as needed. Your device has been removed from Junos fusion.

NOTE: The device uses a factory-default configuration after the Junos OS installation is complete.

Upgrading an Aggregation Device

When you upgrade an aggregation device to Junos OS Release 22.4R2, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

- 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 thirty six months after the first general availability date and customer support for an additional six more months.

For both 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
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

For more information about 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.

Downgrading from Junos OS Release 22.4

To downgrade from Release 22.4 to another supported release, follow the procedure for upgrading, but replace the 22.4 `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.

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.

What's Changed in 22.4R3-S1

IN THIS SECTION

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

General Routing

- **Non-revertive switchover for sender based MoFRR**— In earlier Junos releases, source-based MoFRR ensured that the traffic reverted to the primary path from the backup path, when the primary path or session was restored. This reversion could result in traffic loss. Starting in Junos OS 22.4R3-S1, source-based MoFRR will not revert to the primary path, i.e. traffic will continue to flow through the backup path as long as the traffic flow rate on the backup path does not go below the configured threshold set under `protocols mvpn hot-root-standby min-rate`.

  See min-rate

- **Show active forwarding session for sender based MoFRR**— The `show multicast route extensive` command will show the active forwarding session in the case of source-based MoFRR. The field Session Status: Up and Forwarding will indicate that the particular session is currently forwarding traffic.

  See show multicast route.

VPN

- **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

What's Changed in 22.4R3

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.

General Routing

- **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.]

- 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.

- 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.

- **Multicast debug information added in EVPN options to request system information command (MX Series, QFX Series)**—The output from CLI command `request support information evpn-vxlan` now includes additional information to help debug EVPN multicast issues.

  [See request support information.]

- **Increased maximum limit for TTP TLVs (MX Series)**—The Junos Kernel now accommodates an increased number of TTP TLVs (TNP Tunneling Protocol: type, length, and value messages) to help avoid dropped packets.

  [See show system statistics]

- **Two new alarms are added and can be seen with MPC11E when 400G-ZR optics are used**—High Power Optics Too Warm: warning of the increase in chassis ambient temperature with no functional action taken on the optics Temperature too high for optics power on: New inserted optics when the chassis ambient temperature is elevated beyond the threshold will not be powered on and would need to be reinserted when the ambient temperature is within the acceptable range.

- The packet rate and byte rate fields for LSP sensors on AFT (with the legacy path) have been renamed as jnx-packet-rate and jnx-byte-rate and is in parity with the UKERN behavior. Previously, these rate fields were named as packetRate and byteRate.

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).]

- **Ability to restart restart daemonized applications**--Use the `request extension-service restart-daemonize-app <varname>application-name</varname>` command to restart a daemonized application running on a Junos device. Restarting the application can assist you with debugging and troubleshooting.

  [See request extension-service restart-daemonize-app.]

Network Management and Monitoring

- **Changes to the NETCONF server's `<rpc-error>` element when the `operation="delete"` operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the `<rpc-error>` response that the NETCONF server returns when the `<edit-config>` operation uses `operation="delete"` to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the `<rpc-error>` element includes the `<error-tag>data-missing</error-tag>` and `<error-type>application</error-type>` elements.

- **Changes to the RPC response for `<validate>` operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server emits only an `<ok/>` or `<rpc-error>` element in response to `<validate>` operations. In earlier releases, the RPC reply also includes the `<commit-results>` element.

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.]

- 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

- Prior to this change the output of the "show isis spring flex-algorithm | display xml" command was invalidly formatted when multiple flex algorithm instances were configured. With the change, the XML output is properly structured showing flex algorithm information for each instance. A new XML tag "isis-spring-flex-algorithm" is added to bundle information for each instance.

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 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.

General Routing

- Percentage physical-interface policer is not working on AE, after switching between baseline config to policer configuration. PR1621998
- In a scaled setup with LDP over RSVP configuration and maximum-ecmp as 32 or 64, line card CPU usage can remain high for extended duration on link flap operation. In this duration, LACP might take 5+ minutes to converge and the AE bundle to be active. PR1624219
- On all Junos platforms, agentd process crash will be seen in telemetry streaming longevity test.PR1647568
- If proper gap is given between channelisation and dechannelisation the issue is not seen. Proper gap means allowing the system to complete the previous config before we load the new config. Recommendation is to if we give channelisation config commit wait for the links to come up or atleast the ifd's get created on both evo and RE side and then only revert the config to dechannlisation and vice versa. PR1665625
- VM host snapshot recovery is not enabled for RE-S-X6-128G-K. PR1674091
- Even though GRES is enabled. show system filesystem encryption status command display information about the specific Routing Engine only.PR1674373
- For IPv6 traffic that is ingressing into an Abstract Fabric (AF) interface via MPC11e card, and also sampled, the OutputIntf in the flow records may not be captured if nexthop-learning knob is not enabled. PR1680873
- MVRP on PVLAN promiscuous port is not supported. If MVRP is configured on promiscuous port, then hosts connected to secondary VLAN ports will not be able to reach external world through promiscuous port carrying primary VLAN tags. PR1693345

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. https://kb.juniper.net/TSB18251PR1568757

MPLS

- With local reversion ON, there is a possibility of transit router not informing headend of RSVP disabled link when link is flapped more than once. Work around is to remove local-reversion configuration. PR1576979

Platform and Infrastructure

- On MX and EX9200 serial platforms, under Ethernet VPN (EVPN) environment, packets routed using IRB interface could not be fragmented due to media maximum transmission unit (MTU) problem. PR1522896
- When the "deactivate services rpm" and "deactivate routing-options rpm-tracking" clis 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
- On Mx platforms, VPLS flood traffic loss is observed if flood composite next-hops are out-of-sync on ingress and egress FPCs during transport path revertion.PR1656216

Routing Protocols

- When "routing-options transport-class fallback none" is not configured - do not configure more than 10 transport-classes. Or advertise more than 10 distinct colors in SRTE or FlexAlgo. This limitation will be fixed by PR-1695020. PR1648490

Services Applications

- In release 17.4 and forward, subscriber sessions on the LNS that send an ICRQ that includes RFC5515 AVPs may fail to establish a session. The client will receive a CDN error "receive-icrq-avp-missing-random-vector" in response. PR1493289

What's Changed in 22.4R3-S1

IN THIS SECTION

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

General Routing

- **Non-revertive switchover for sender based MoFRR**— In earlier Junos releases, source-based MoFRR ensured that the traffic reverted to the primary path from the backup path, when the primary path or session was restored. This reversion could result in traffic loss. Starting in Junos OS 22.4R3-S1, source-based MoFRR will not revert to the primary path, i.e. traffic will continue to flow through the backup path as long as the traffic flow rate on the backup path does not go below the configured threshold set under `protocols mvpn hot-root-standby min-rate`.

  See min-rate

- **Show active forwarding session for sender based MoFRR**— The `show multicast route extensive` command will show the active forwarding session in the case of source-based MoFRR. The field Session Status: Up and Forwarding will indicate that the particular session is currently forwarding traffic.

  See show multicast route.

VPN

- **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

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.

Class of Service (CoS)

- While Traffic control profile is with only scheduler map associated with it and if its attached to IFL , commit error to be thrown. PR1688790

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
- On all platforms, MAC-IP route deletion and addition are triggered when re-ARP (Address Resolution Protocol) on MH (Multihoming) device fails in the EVPN-MPLS multihoming scenario resulting in traffic drop. PR1691132

Forwarding and Sampling

- On MX series routers which support MPCs (Modular Port Concentrators), the ingress-queue-filter was not programmed correctly causing the traffic loss. The issue is seen only on non zero PFE (Packet Forwarding Engine) interface. PR1751494

General Routing

- AFEB crashing with PTP thread hog on the device. PR1068306
- 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
- When there is an input failure on one of the AC PEMs (low or high) it's wrongly categorized as a "Mix of AC PEMs". Thus, instead of "PEM input failure" an alarm "Mix of AC PEMs" might be raised.PR1315577

- On WRL8 based VMHost platforms (i.e., ACX6360/PTX10001/MX150/NFX150/NFX250/NFX350), there is no log rotation for resild log and temperature sensor info is incorrectly written into resild log which could result in continuous logs in resild log file. The disk usage might keep increasing due to this issue. The disk usage could be eventually full which could cause system to hang and reboot. PR1480217

- When there are HW link errors occurred on all 32 links on an FPC 11. Because of these link errors, all FPCs reported destination errors towards FPC 11 and FPC 11 was taken offline with reason "offlined due to unreachable destinations". PR1483529

- After backup Routing Engine halt, CB1 goes offline and comes back online; this leads to the backup Routing Engine booting up, and it shows the reboot reason as "0x1:power cycle/failure." This issue is only for the RE reboot reason, and there is no other functional impact of this. PR1497592

- In the platform using INH (indirect next hop, such as Unilist) as route next hop type for multiple paths scenario (such as BGP PIC or ECMP), the session fast-reroute might be enabled in Packet Forwarding Engines (PFEs). When the version-id of session-id of INH is above 256, the PFE might not respond to session update, which might cause the session-id permanently to be stuck with the weight of 65535 in PFE. It might lead PFE to have a different view of Unilist against load-balance selectors. Then either the BGP PIC or the ECMP-FRR might not work properly and traffic might be dropped or silently discarded. PR1501817

- PR1463859 introduces a software defect that causes a 10GE interface to flap continuously when configuring with the WAN-PHY framing with the default "hold-down" timer (0). Once upgrading a router to an affected software release, the interface may flap continuously. This is not applicable to an interface with the default framing - LAN-PHY. PR1508794

- When launching a guest Virtual Machine (VM) to run a third party application on Junos OS 15.1R1 and above, the guest VM might be shown as "UNAVAILABLE" even after successfully installing the third party application. This is due to duplicated device ID assigned to different disks. PR1529596

- Due to BRCM KBP issue route lookup might fail. Need to upgrade KBP to address this issue, Due to high risk KBP SDK upgrade planned for 21.1. PR1533513

- USF-SPC3 : With ipsec PMI/fat-core enabled, "show services sessions utilization" cli not displaying right CPU utilization. PR1557751

- 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

- Service MIC does not work on ACX500 running Junos 20.4 or higher. PR1569103
- 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
- Service MIC does not work on ACX500 running Junos 20.4 or higher. PR1569103
- 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
- On QFX5110 VC, FPC may gets disconnected with 24K DHCPv6 relay scaling, after the traffic is stopped. "pfe_listener_disconnect" error messages may be seen.PR1594748
- 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 lower than 21.3R1. PR1597276
- During RE switchover, if there is a burst of ICMP/BFD/SSH/FTP/TELNET/RSVP packets (~18K pps) you might see new backup RE restarting. PR1604299
- On MX-VC (Virtual Chassis) platforms with MS-MPC or SPC3 service cards and AMS(Aggregated Multi-Service), traffic on the line card in the backup chassis may not be load-balanced properly due to timing conditions. This works well on the line card in the master chassis. There might be traffic loss when interfaces are not properly balanced.PR1605284
- output of show network agent command should be null, which shows statistic per component after GRES. PR1610325
- When user tries to disable AMS ifd using config knob, the ipsec tunnels are not deleted. Deactivating the services will provide the desired result. PR1613432
- On all Junos platforms the MAC address of the 17th ae interface might be changed after the upgrade from 18.4+ to 20.4+ releases. It will lead to mac based service interruption.PR1629050
- The fabric statistics counters are not displayed in the output of "show snmp mib walk ascii jnxFabricMib". PR1634372
- On all devices running Junos OS or Junos OS Evolved, where this is a high BGP scale with flapping route and the BGP Monitoring Protocol (BMP) collector/station is very slow, the rpd process might crash due to memory pressure. PR1635143
- 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

- vMX: "input fifo errors" drops reported under pfe shell "show ifd" but not seen in "show interface extensive" output. PR1642426
- The broadband device has to be manually enabled in the configuration for DHCP and PPP access models for BNG CUPS. Configuration to enable the bb device is as follows: #set system subscriber-management mode force-broadband-device. PR1645075
- On Junos platform, PTP does not lock when port speed is not configured under PIC hierarchy or port speed for some additional random ports are configured under the PIC hierarchy or perform PIC deactivate/activate.PR1645562
- Core dump reported intermittently where random grpc stack crash is observed. The license service will auto restart and recover.PR1656975
- On Junos platforms, in the VPLS environment when having "routing-options resolution preserve-nexthop-hierarchy" configured results in the packet dropped at egress PE for multiple MPLS stack labels.PR1658406
- The OpenSSL project has published security advisories for multiple vulnerabilities resolved in OpenSSL. Please Refer to https://kb.juniper.net/JSA70186 for more information.PR1661450
- With following configuration changes subscribers are coming up. Config changes: ========== set forwarding-options dhcp-relay overrides allow-snooped-clients set forwarding-options dhcp-relay group DHCP-FO overrides allow-snooped-clients set forwarding-options dhcp-relay group DHCP-FO overrides user-defined-option-82 100.112.77.66 deactivate forwarding-options dhcp-relay group DHCP-FO interface ae31.0 overrides. PR1665499
- On all Junos and Junos Evolved platforms, the user should not modify the locator attributes, instead, locator, SIDs should be deleted and configured back. Otherwise, it will lead to core file.PR1667320
- On MX platforms with MIC-MACSEC-20GE, FEB(Forwarding Engine Board) may go down while activating/deactivating GRES (Graceful Routing Engine Switchover) configuration.PR1668983
- These are expected error logs, and doesn't cause any functional impact. "jsr_iha_pri_unrepl_msg_func: Error: Invalid primary handle in msg 0x10006c600000621, error=2" These logs might be seen if the following conditions are met: * On all Junos OS platforms * Non stop routing is enabled. * with scaled setup The possible triggers would be restart chassisd, ksyncd, switchover, re reboot... which causes nsr unreplication/replication.PR1675057
- Sometimes cores are reported on backup RE during init after a reboot etc. When the backup RE initialization is being done and system is busy, some commands executed in context of spmbpfe are taking more time to complete due to the initial heavy lifting by the kernel, In this stage, if in case the commands from spmbpfe process do not complete for >2.5 seconds, then there are chances of

spmbpfe cores. This is a temporary issue seen on backup RE during init time only. This may not be impacting because if in case spmbpfe process crashes due to this, it would restart by itself and continue to init and run once the initial high cpu condition has passed. It should not cause any functionality or performance impact; especially since it is reported only on backup RE.PR1675268

- On LC480 MX line-card with 1G interface 1PPS time error does not meet class B requirement (maximum absolute time error is 70 ns).PR1677471
- A new command has been introduced that will display the differences between the destroute entries learned within l2ald and present in the kernel. PR1677996
- 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
- Changing a filter from interface-specific to physical-interface-filter (or visa versa) while also restarting the firewall process may result in issues with LACP. To avoid this, deactivate the filter before changing the mode.PR1679965
- 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
- With this the maintenance-domain (MD) configuration and maintenance-association (MA configuration) under the connectivity-fault-management stanza will be ordered by the system and not as per the configuration order. PR1682939
- When the hostname configuration is changed, the change is not reflected in the RIFT output. Also when changes are made to the REDIS configuration, they are not applied until rift is restarted via "restart rift-proxyd". PR1686233
- On all Junos and Junos Evolved platforms if MVRP (Multiple VLAN Registration Protocol) is configured on an MSTP (Multiple Spanning Tree Protocol) enabled interface, the interface will be made part of all the existing MSTI (Multiple Spanning Tree Instance) on the switch and it will take part in the FSM (Finite State Machine) of all the MSTIs. If this interface will go into the forwarding state for the MSTI, of which it is not a part actually, will result in dropping in traffic of that particular VLAN.PR1686596

- 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
- With Sharding enabled, BGP flags like the following are not displayed on Active route in "show route extensive" output:"Accepted Multipath MultipathContrib MultiNexthop" Per shard view, using "show route extensive prefix rib-sharding shard-name" will show these flags.PR1693207
- Issue is seen when multiple line cards exports telemetry data for sensor-path "/junos/system/linecard/fabric/" and one of the line card exporting data reboots. After rebooting, the same card or one/more cards may stop streaming of data or streaming of data will be too slow to detect. Removing one or more line card from telemetry streaming of this data resolves the issue.PR1693394
- It is recommended to use IGP shortcut with strict SPF SIDs in SRTE path. if Strict SPF SIDs are used then this issue would not occur. This issue will occur only if regular ISIS SIDs are used in SRTE path and IGP shortcut is enabled. with this, if customer perform multiple times deactivate/activate for SRTE telemetry. PR1697880
- During BGP MP route 9.0.0.2 re-resolution window, a corner case was hit, such that rpd will assert and restart. This error case is observed 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. This issue will get resolved in next 22.4R1 services releases.PR1699773
- Once the device is loaded with the new image, PIC tries to boot up. mspmand is one of the processes inside PIC, crashes sometimesPR1700462
- The optic configuration mismatch alarm was always enabled, but was not reported by the RE during 'show chassis alarms'. This alarm will now be correctly reported by the FPC and displayed in the RE. There is no behavior change other than the alarm being reported correctly now.PR1700606
- On Junos platforms, even though there are no active subscribers, a foreign file propagation (ffp) commit error is seen for the class-of-service traffic-control-profile.PR1700993
- 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
- In Chassisd, Jvision thread takes more time in streaming of jvision 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 RE, which eventually was causing automatic RE 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

- On Junos 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 the MX104 platform, the Wrong threshold-temperature is displayed.PR1713788
- On Junos MX10008 platform, the FPC (Flexible PIC Concentrator) crash will be observed when connected to non-Juniper SFP (Small Form-factor Pluggable) and it will lead to traffic loss.PR1722823
- On all Junos and Junos Evolved platforms BGP traceoptions configuration will have an impact on the CPU, threads will be busy and will take time to recede in spite of disabling it. It is important we enable a specific trace flag and disable it when the CPU goes high. It is also important not to perform switchover and other triggers which can add load to the CPU during traces are enabled. Traces must be enabled discretely. PR1724986
- MX304 Major Alarm " Host 0 detected AER correctable error" after RE switchover.PR1731237
- gNOI "Rotate" and "Install" gRPC message should be handled as part of a single RPC stream instead of individual RPC message. Currently, each message in rotate and install RPCs are handled as separate stream. If the same stream is used to send multiple RPC messages, the rotate gRPC will fail.PR1732601
- Xmlproxyd crash could be seen if there are multiple collectors subscribing for Xmlproxyd sensors and some or all of the collectors are flapping frequently at the rate of 90 seconds or so. The occurrence of this issue is rare. The telemetry streaming of Xmlproxyd sensors will be absent during the time Xmlproxyd crashes and restarts on its own. This time could be within 30 seconds or so. Once Xmlproxyd comes up, the telemetry streaming of Xmlproxyd sensors will be resumed automatically.PR1732763
- 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 100Gbps10g Sets the interface mode to 10Gbps200g Sets the interface mode to 200 Gbps25g Sets the interface mode to 25Gbps400g Sets the interface mode to 400Gbps40g Sets the interface mode to 40Gbps50g Sets the interface mode to 50GbpsPR1734654
- On all Junos devices, the time needed to commit increases when a Trusted Platform Module (TPM) is configured.PR1738193

- On all Junos and Junos Evolved platforms, in a rare scenario, the FPC will go down due to core.PR1739595
- When running DHCPv6 Relay in CUPS model, on UP GRES DHCPv6 traffic loss is observed.PR1743087
- The switch-options settings on logical-system will be not reflected after Routing Engine rebooting or Routing Engine switchover. This will happen logical-system only. In default instance, this behavior cannot be seen. PR1743737
- RPD core is sometimes seen if there are many unilist nexthop with identical key values but different metric in Evo, esp when ACK is requested for those nexthops.PR1745509
- 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
- Memory in VMhost level is still in cache and not properly freed after take VMhost snapshot. PR1755585

High Availability (HA) and Resiliency

- When GRES is performed with the interface em0 (or fxp0) disabled on the primary Routing Engine, then enable the interface on the new backup Routing Engine, it isn't able to access network.PR1372087

Infrastructure

- A Use After Free vulnerability in the kernel of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). Refer to https://kb.juniper.net/JSA70198 for more information. PR1636063

- NTP time drift on the affected Junos releases. Earlier implementation of kvmclock with vDSO (virtual Dynamic Shared Object) which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate.PR1691036

Interfaces and Chassis

- MediaType value in SNMP/Jvision is not correct for DOWN interfaces after the switch comes up following a reboot. PR1671706
- IFL packet counters are not implemented for AMS interface. It is a new change. PR1673337
- This issue is specific to MXVC only and the issue is not seen during manual execution of the test case. Issue is seen only with the test script that too rarely and hence the exact trigger of the issue is not clear. PR1686425
- On all Junos platforms, if a speed mismatch happens in the LAG (Link Aggregation) and member interface then a traffic drop will be seen.PR1725168

J-Web

- PHP software included with Junos OS J-Web has been updated from 7.4.30 to 8.2.0 to resolve multiple vulnerabilities. Please refer to https://supportportal.juniper.net/JSA71653 for more information. PR1698386

Layer 2 Features

- In case of the access-side interfaces used as SP-style interfaces, when a new logical interface is added and if there is already a logical interface on the physical interface, there is 20--50 ms traffic drop on the existing logical interface. PR1367488
- On all Junos Evolved and Junos MX platforms, when a new logical interface(LSI) is created, but the configuration was deleted as the kernel failed to add the interface will lead to rpd crash.PR1680687
- in a H-VPLS network with VPLS hot-standby and the knob '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

Layer 2 Ethernet Services

- If a client sends a DHCP request packet, and option 55 includes PAD option (0), a DHCP ACK will not be sent back to the client. PR1201413
- In the CBNG (XDA CUPS) environment, DHCPv6 subscribers fail to login over PPP over L2tp Tunneled. This setup has XDA CP and UP for both LAC and LNS. DHCPv6 subscriber is stacked over PPP from the Client side. While the PPP(v4 and v6) session gets established successfully, DHCPv6 subscriber traffic is being dropped at the LNS UP. Though this is the Release notes for 22.4R1 Release, issue is not seen in 23.1 based Dev Common Branch. Adding the release notes for 22.4R1 scope only. PR1683955
- DHCP ALQ no-advertise-routes-on-backup functionality does not work in VRF for Framed-Route. PR1740822

MPLS

- ingress will retry after lsp stay down for extended period of time or customer can clear lsp to speed up the retry. PR1631774

Network Management and Monitoring

- In some NAPT44 and NAT64 scenarios, Duplicate SESSION_CLOSE Syslog will be seen. PR1614358

Platform and Infrastructure

- PVSTP protocol packets is getting duplicated when it tunnelled through Layer2 tunnelling protocol. Other protocol data units PDUs(STP,VTP,CDP) are not impacted. PR1686331
- On Junos MX platforms, when Virtual Router Redundancy Protocol (VRRP) packets come from the LAG interface with delegate-processing enabled, it should be processed on anchor PFE. If it comes from non-anchor PFE - it goes to anchor PFE through the fabric. In that case, TTL is decremented. If a FW filter on the loopback interface is applied for VRRP with a ttl=255 condition, the VRRP won't work - there will be a service impact.PR1701874
- On Junos MX and EX92XX with specific line cards, VLAN rewrites will not happen for traffic egressing from IRB(Integrated Routing and Bridging) interface over an L2 AE (Aggregated Ethernet)

IFL (Interface Logical), if the L2 AE IFL is configured to perform VLAN rewrites on the frames. This happens when the IRB is configured as a routing-interface on EVPN (Ethernet Virtual Private LAN) or VXLAN (Virtual Extensible LAN) routing instances and the traffic has to egress on IRB over an L2 AE IFL. As a result, the frames are forwarded with incorrect VLAN tag information.PR1720772

- On Junos MX platforms, in Ethernet Virtual Private Networks-Layer 2 Virtual Private Networks-Circuit Cross-Connect (EVPN-L2VPN-CCC) setup, the integrated routing and bridging (IRB) interface over access logical tunnel (LT) interface is configured, it is sending vlan tagged packet on the access port and not removing it causing the host communication to break.PR1740606

Routing Policy and Firewall Filters

- On all Junos and Junos OS Evolved platforms where Openconfig routing policies are configured, deleting a single prefix from prefix-list deletes all the prefixes.PR1691218

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 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

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

- BGP LU statistics does not report correct statistics when sharding is enabled. This is not specific to BGP CT feature of this RLI. This will be fixed via RLI 53922 [Umbrella RLI to fix small Topgun Sharding Gap]. PR1684238
- 22.3 onwards, isis yang is uplifted to 1.0.0 version which has major change in existing OC path that was supported earlier. Since OC path has change, same need to reflected in translation script which is not done. As part of D27 release for cloud, translation script will be modified with newer OC path. Till then supported older OC config is broken. eventually D27 code will come back to DCB and things will work fine after that. PR1686751
- The issue is not addressed for 22.1R3 and will be addressed in future releases. PR1687273
- This issue is seen with only evo and not seen Junos. Its seen in a combination of Rsvp and ISIS. Stats is getting incremented. PR1700063
- On all Junos and Junos OS Evolved platforms with dual-RE, after back to back Graceful Routing Engine switchover (GRES) is performed, the periodic packet management process (ppmd) crash will be seen. PR1702687
- On all Junos and Junos Evolved platforms with TI-LFA (Topology-Independent Loop-Free Alternate) feature enabled, when IP address is removed from one interface and is assigned to another interface in the same commit, the rpd process crashes affecting routing control plane. PR1723172

Services Applications

- When a configured tunnel interface is changed to another one, flow-tap-lite functionality stops working i.e, packets don't get mirrored to content destination. But, this problem isn't consistently seen. PR1660588

User Interface and Configuration

- On all Junos OS Evolved platforms, when archiving configuration files to a remote IPv6 host using Secure Copy Protocol(SCP), file transfer fails.PR1720525

VPNs

- When using Group VPN, in certain cases, the PUSH ACK message from the group member to the group key server may be lost. The group member can still send rekey requests for the TEK SAs before

the hard lifetime expiry. Only if the key server sends any new PUSH messages to the group members, those updates would not be received by the group member since the key server would have removed the member from registered members list.PR1608290

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.

Application Layer Gateways (ALGs)

- The traffic will be dropped in the DS-Lite+ALG scenario. PR1715315

Authentication and Access Control

- Connection fails are observed on Junos despite a valid auth entry. PR1692398

Class of Service (CoS)

- The cosd process crash might be seen on all Junos platforms. PR1719028
- Cos Scheduling hierarchy on PS interface is destroyed when the TCP is modified. PR1722939
- The cosd could crash due to upgrade to 21.2R3-S4 with AE specific wildcard and explicit configuration. PR1725769
- 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

EVPN

- A high CPU consumption of mcsnoopd process is seen under IGMP-snooping configured scenario leading to its crash. PR1713508
- Ping overlay vxlan replies Overlay-segment present even the bridge-domain has been deactivated. PR1715343
- RPD process crash might be observed when routing or evo-pfemand process is restarted and multicast snooping process adds a route to inetmcsn.1 table. PR1716663
- 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
- The rpd core is seen in the long-running devices with EVPN enabled. PR1723832
- 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

Forwarding and Sampling

- The Firewall filter with syslog action will not work when applied on the ingress of a loopback interface. PR1714988
- Traffic is leaking during a filter change. PR1715504
- FPC cards restart unexpectedly. PR1743032
- High CPU utilization of the mib2d process will be observed with error messages due to stale SNMP requests. PR1749092

General Routing

- The LSI interfaces are not created after the device reboot. PR1690105
- Continuous Deactivate/activate of security configuration can lead to process restart. PR1566044
- 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
- PTP Playback Engine reset error is reported sporadically with PTP FPGA Firmware version A4 7. PR1652275
- Images older than 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
- MPC11E temperature alarms with 400G-ZR optics. PR1663175

- MX10008/MX10004: Constant logs of "Array too small" logs in chassisd. PR1672078
- 100GE interface on JNP-MIC1 TIC module may keep flapping for 1 ~ 45 minutes after a specific 3rd party peer device (NRU02 from Arista/Pluribus) is booting up. PR1686012
- With the logout-on-disconnect configuration, the prompt for setting the root authentication password on the console will not appear. PR1686364
- New CLI commands addition to support RE and Chassis power-cycle. PR1686577
- The pre-installed optional packages and JSUs will be lost after a VMHost rollback. PR1686825
- xml validation failure seen for "show security macsec connections | display xml validate" with ERROR: Duplicate data element. PR1691435
- On all Junos lsys systems RPD process crashes due to JET client invoking rpc handled by RPD daemon. PR1692738
- The rpd crash will be observed when there is a temporary recursion loop and routes are flapping. PR1692776
- Context deadline exceeded observed on while adding NH , IPv4. PR1693567
- 22.4R1::JVISION:: "[01;31m[KFPC3:NPU0[m[K" string is missing in Npu memory after jvision exports data. PR1696021
- Dynamic Tables stuck in KRT Queue. PR1696199
- Transceiver not detected after it's unplugged and plugged in again. PR1696444
- Traffic loss can be seen while switching between primary and fallback sessions in MACsec setup. PR1698687
- The kernel crash can be seen in the VPLS scenario. PR1698781
- DHCP offer requests are dropped while routed towards different VRFs of transit router. PR1700203
- VLAN tags are imposed incorrectly when traffic is routed over IRB going out of the access interface. PR1700321
- FPC crash is observed and the device is rebooted when multiple interface operations are performed in MX platforms with LC480 linecard. PR1700909
- Power supplies in the output "show chassis environment" are showing as present state where atleast one is expected to be in OK state. PR1701240
- The rpd crash will be observed when there is a temporary recursion loop and routes are flapping. PR1692776

- PDT: ONDATRA: context deadline exceeded observed on while adding NH , IPv4. PR1693567
- 22.4R1::JVISION:: "[01;31m[KFPC3:NPU0[m[K" string is missing in Npu memory after jvision exports data. PR1696021
- Dynamic Tables stuck in KRT Queue. PR1696199
- Transceiver not detected after it's unplugged and plugged in again. PR1696444
- Traffic loss can be seen while switching between primary and fallback sessions in MACsec setup. PR1698687
- The kernel crash can be seen in the VPLS scenario. PR1698781
- DHCP offer requests are dropped while routed towards different VRFs of transit router. PR1700203
- VLAN tags are imposed incorrectly when traffic is routed over IRB going out of the access interface. PR1700321
- FPC crash is observed and the device is rebooted when multiple interface operations are performed in MX platforms with LC480 linecard. PR1700909
- Power supplies in the output "show chassis environment" are showing as present state where atleast one is expected to be in OK state. PR1701240
- CB2 not properly offlined upon Power Zone Failure. PR1701539
- Some PPPoE subscriber connection lost during RE switchover. PR1701739
- The xmlproxyd process crash is observed in telemetry scenario. PR1702250
- Updated "show l2-learning vxlan-tunnel-end-point remote" now displays svtep for multiple routing instances. PR1703412
- Alarms for PEMs are still seen when PEM are removed from the chassis. PR1703566
- The line card abruptly reboots when ISSU is performed. PR1703910
- RPD core@bgp_rt_terminate_job->bgp_process_rt_terminate->bgp_rt_terminate_subr->bgp_rto_adv_q_free (). PR1704393
- Interface flaps are seen after PTP GM changes to a different FPC slot. PR1704633
- Silent drop in traffic in the event of a link failure (Rx LOS) for 1GE-SX/LX optics. PR1705461
- No network reachability when enabling the routing-service knob for PPPoE subscribers over AE. PR1706446

- The FPC crash can be seen on QFX5k platforms during simultaneous soft and hard OIR of SFP. PR1707094
- VMX :: JUNOS-REG: VMX: PFE syslog tags are missing for the command help syslog "^PFE_?" PR1707504
- Upon ISSU upgrade or system reboot or FPC restart the DAC 100G speed configured port might not come up. PR1707976
- CLI command 'show snmp mib walk ascii' is not showing the correct output for jnxSubscriberPicCountTable and jnxSubscriberSlotCountTable. PR1709029
- ICCP connection establishment b/w JUNOS and EVO is not supported. PR1710448
- No alarm is raised when PSU is inserted with different airflow directions. PR1710952
- gNMI line card (PFE) sensor /junos/system/linecard/packet/usage/ may have packet drops (gNMI translator lookup failures). PR1711779
- Master and Backup RE synchronization issue will be seen if chassisd is restarted on Master RE. PR1712352
- PCT : Show Ephemeral-Configuration Instance Junos-Analytics is not giving expected output while verifying the commit operation with new config hierarchy openconfig-telemetry:telemetry-system. PR1712409
- The MACsec on the channelized IFD impacts the MACsec traffic on other channelized IFL interfaces within the same port and vice versa. PR1712554
- Next-hop programming issue at PFE on Junos PTX and QFX10k platforms when the member of unilist is in hold state. PR1713279
- The rpd process will crash when BMP is configured. PR1713444
- The member interface will not be added to the AE bundle if the link-speed of the AE interface doesn't match that of the member.. PR1713699
- IPv6 Fragmentation is not working on MS-MPC/MS-MIC in DS-Lite scenario. PR1713725
- Unexpected load balancing of packets having GRE header. PR1713958
- Subscribers connectivity is lost due to multiple MIC restart on all Junos MX platforms with MPC5E and BBE configuration. PR1713968
- Traffic loss is seen on telemetry streaming in BGP sharding environment. PR1714087
- PPPoE and DHCP subscriber connection on dynamic VLAN can fail on Junos MX platforms. PR1714778

- PTP statistics will not be visible after RE switchover. PR1715314
- The agentd would become unresponsive on all Junos platforms. PR1715377
- The bbe-smgd process is seen to crash if a large scale PWHT configuration is present. PR1715410
- Known multicast traffic is not forwarded when MLD snooping is enabled. PR1715429
- Untagged packets get dropped while adding a layer 3 logical unit to an interface with native vlan configured. PR1715477
- Traffic loss is seen on RTG bound interface. PR1715518
- BMP station will not receive the RIBs as expected. PR1715886
- After the device reboots with lpm(longest prefix match) profile configured, the default route entry is getting created on ipv4 and ipv6 (pfe hw lpm) due to gRIBI routing instance and same route is removed after the interface flap. PR1715907
- Memory leak will be observed in rpd after performing restart routing. PR1716431
- Traffic loss due to incorrect route resolution and KRT queue getting stuck with 'EINVAL -- Bad parameter in request' error. PR1716436
- The link remains down on connecting the transceiver 10GBASE-T with the serial number starting with "2P1". PR1716703
- J-flow sends wrong IP in sampling records when NAT is configured for traffic along with input sampling. PR1716707
- A 10G port on a MPC2E or MPC3E 4x10G MIC can randomly flap constantly every few seconds. PR1716766
- SNMP MIB OID output showing wrong temperature value if device running under negative temperature. PR1717105
- Traffic loop is seen due to incorrect root bridge ID. PR1717267
- FPCs will be stuck at maximum CPU utilization when Nextgen statistics thread is hogging the CPU. PR1717621
- In a DHCP ALQ subscriber scenario delete-binding-on-renegotiation knob does not work as expected due to a synchronization error between the primary and the backup routers. PR1718342
- RPD cores when routing churn happens, if RE restart was missed after configuring FMBB knob. PR1718510
- mx2010::DVAITA-SUBLC: Fabric plane on few PFEs assigned to SLC shows as unused. PR1718834

- The PPTP connection itself won't work when trying to establish PPTP connection along with DSLITE. PR1718840
- Same MAC address is assigned to CBP and GE interface instead of being unique on MX304. PR1719084
- The subscribers will be stuck in a terminated state when an FPC is taken offline. PR1719427
- Major Host 1 Chassis Manager connection down Alarm on MX304. PR1719767
- 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
- Convergence delay is seen when FPC is offlined under heavy traffic and scaled scenario. PR1719956
- The existing DHCP server bindings will be lost after configuring the additional group in the dhcp-local-server bundle. PR1720002
- The rpd process crash will be observed while creating/updating the PCEP tunnel. PR1720031
- Reachability loss between Master and backup RE in certain condition on MX2008 platform. PR1720407
- In a rare case FPC crashes and reboots generating a core. PR1720591
- 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
- The dcpfe process crash will be observed in the EVPN-VXLAN multihoming scenario. PR1721322
- BFD session failed when configured on the loopback sub interface. PR1721714
- The filter will not work as configured upon changing the "physical-interface-policer" parameters. PR1722776
- Router Send RA with Router lifetime 0 when the upstream interface is shut. PR1722809
- PADT response will not be sent for an incoming PPPoE/PPP data Packet from an unknown session ID. PR1722945
- Complete traffic blackhole from one PFE to another on fabric links after injecting/reporting CRC errors on fabric links of MX10008. PR1724007

- On certain Junos MX platforms with SCB3 SyncE fails after enabling PTP. PR1724254
- PS interface remains up while LT or RLT interface is down. PR1724298
- The "show mac-vrf flood vlan-name" is changed to "show mac-vrf flood 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 command reports APM not connected when in fact it is connected. PR1725143
- The error logs "fpc0 expr_hostbound_packet_handler: Receive pe 254?" would be generated. PR1725716
- PTSP subscribers are stuck in 'configured' state. PR1726136
- Enabling disk smart-check utility on the routing-engine with Innodisk SSD raises a false positive smart error. PR1726252
- JSU installation fails when MACsec is configured. PR1726264
- Root user is unable to login using public key authentication after reboot or upgrade. PR1726621
- Traffic drops with percent policer attached using list. PR1726733
- 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
- FPC crash observed when the ASIC usage is high. PR1727427
- 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

- 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
- [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
- 23.2R1 :USF_DNSF:log messages are not generated when Sending MX query with domain name in black list with action as report after configure the web filtering with one/morep profile and template. PR1733435
- 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
- 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
- Silent trop in traffic will be observed when the SR-TE shortcut is configured. PR1737119
- URL-Filtering few HTTP sites are getting bypassed and redirect is not happening. PR1737670
- PSoRLT Aggregate Stats: ipv4 leaf elements for ps transpfort ifl are exported , since ps is l2 interface no stats under ipv4 should be exported,. PR1737935
- Eventd running 100% CPU cycle while running AMS statistics related show command continuously. PR1738300
- 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
- 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
- SPMB process will crash and PICs will not come online. PR1742186
- Tunnel interfaces are getting bounced causing a momentary impact on traffic. PR1742510
- The l2ald crashes when there is recursive deletion of IFBD or when BGP neighborship is cleared in EVPN-VXLAN multi-homed configuration. PR1743282
- Due to SPMB restarts in the middle of the FPC boot process, FPC wont come up. PR1743686
- The picd process crashes when executing the CLI command "show service sessions/flows" or "clear service sessions/flows". PR1743031
- 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
- Enhancement of PoE controller firmware files into Junos Software. PR1745088
- MPC10E - PIC bounce/config change on a PIC with 10G QSA adaptor can cause a FPC restart. PR1745317
- The rpd crashes when BGP sharding, multipath and dynamic tunnel are configured. PR1746012
- PTP master feature will not work as expected. PR1746984

- MPC10E line card crashes when it reboots after FPC firmware upgrade. PR1746541
- Traffic from subscribers will be dropped by Junos based MX 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
- MX2k Platform: frequent fabric plane Check state reported due to remote destination timeouts. PR1747893
- JDI-RCT: SMVS2.0-ISIS-SR: RPD crash observed @0x0000000002456944 in krt_flow_rth_q_handler (kqp-optimized out, isflash-optimized out, todo-optimized out, krt_state_old-optimized out) at ../../../../../../../../src/layer3/usr.sbin/rpd/lib/krt/krt_flow.c:6518" with test configs. PR1749252
- Connectivity fails intermittently on 802.1x enabled ports. PR1749312
- PFE Flow ID doesn't shows correct in "show subscriber extensive" output. PR1749336
- For OSPFv3 interoperability issue between Junos and Junos Evolved platforms will be seen with the authentication algorithm hmac-sha-256-128 for IPsec SA. PR1749779
- SyncE stuck in holdover upon PTP slot switchover without change in PTP phase align state. PR1750316
- ARP learning issue for dynamic ARP entry for the DVLAN stacked frame route not resolved. PR1751656
- FPC reboots are observed during unified in-service software upgrade (ISSU) on MX10008/MX10016 resulting in ISSU being unsuccessful. PR1751785
- Service PIC enabled with url-filtering might crash and gets into booting loop. PR1751860
- "ssh root-login allow" is needed to upgrade firmware on MX304. PR1752765
- Traffic impact will be seen for static VoIP VLAN on access interface if same VLAN configured as data VLAN. PR1754474
- Continuous fpc0-aftd-trio coredump on MX304 when turning up ipv6 neighbors with LMIC 2. PR1755950

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 platforms. PR1707707
- On Junos platforms the dcd will flap the IFLs which are part of EVPN routing-instance. PR1712800
- 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
- Issue in VRRP inline adjacency whenever a master router uplink goes down on MX platforms. PR1720943
- PFE table is not updated when new VLANs are added in an AE bundle when ESI is enabled. 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

Layer 2 Features

- The rpd process crash will be observed during VPLS to EVPN migration. PR1729052

Layer 2 Ethernet Services

- On all Junos MX Series and PTX Series routers, multiple LACP timeouts cause traffic loss due to ppman resource starvation. PR1706224
- A jdhcpd process crash is observed on all Junos platforms. PR1713619
- The DHCPv4 relay will send two option-82 to the server and the DHCP session will not be established. PR1714260
- DHCP binding is not happening in EVPN VXLAN topology with DHCP stateless relay (forward-only). PR1722082
- Active bulk leasequery is not working for IPv6 DHCP local server on MX platforms. PR1744162

MPLS

- After disable/enable MPLS, targeted LDP session is not getting established. PR1687834
- The rpd process will crash when rpd is restarted. PR1698889
- Pathtear message is not forwarded by PLR to merge point which is causing data plane blackholing. PR1703424
- Member LSPs of a container LSP will be torn down unexpectedly. PR1705964
- LDP sessions flap when router-id is changed. PR1706064
- PathErr with RoutingProblem error code generated unexpectedly during dual failure local repair. PR1713392
- Routing Engine initiated PING failed over MPLS interface. PR1723145
- 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 blackhole 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

Network Management and Monitoring

- Consistent high CPU usage is seen on the device post reboot. PR1691986
- Syslog messages modification for SNMPv3 authentication failure. PR1734549

Platform and Infrastructure

- JDI-RCT:M/Mx: FPC core @ jnh_call_read_index , trinity_nh_ucast_uninstall_hw. PR1636758
- Disabling PFE triggers the memory leak which might cause FPC to crash. PR1686068
- The vmcore crash observed in low memory conditions. PR1694463
- The TCP sessions for BGP are closed on the backup Routing Engine. PR1700438

- The DEI bit will not be copied in the inner VLAN tag although the incoming traffic has the DEI bit set. PR1714429
- In TWAMP server/reflector, test traffic classified by ingress filter is re-classified by host-outbound-traffic statement. PR1722232
- ksyncd core with dhcp subscribers. PR1722708
- Traffic drop would be observed while restarting the chassis-control. PR1724563
- Traffic loss observed for packets over IRB over LT. PR1724925
- On certain Junos MX platforms queue buffer-size temporal computation is not happening correctly. PR1726698
- 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
- MPC line card reboots when subscriber management services are configured. PR1737615
- 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

Routing Policy and Firewall Filters

- Issue in committing more than 23, 4-byte AS on Junos and Junos Evolved platforms. PR1706143
- The flowd process crash is observed with the security policy updated with changing IP address related to the FQDN. PR1713576
- Commit error will not be seen after deactivating routing-instance applied under firewall filter. PR1720389

- 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

- PPMD crashed at `ppm_destroy_distrib_proto_stats_group_entry ( )`. PR1660299
- More than expected traffic loss is seen with ECMP FRR enabled during link down scenario. PR1687887
- BGP LU Advertisements fail with the message "BGP label allocation failure: Need a gateway". PR1689904
- The BGP neighbor receives the parent authentication regardless of the authentication setup under the neighbor. PR1691299
- The mscnoopd process crash will be observed when snooping configuration is removed. PR1696374
- BGP scheduler slips during sub-optimal prefix-walk while deleting selected prefixes from a large set. PR1696870
- Multicast traffic loss for 2-3sec. PR1698265
- The rpd process might crash when SPF is recalculated. PR1699076
- The mcscnoopd process will be stuck in resync state after snooping configuration is deleted and added again immediately. PR1699784
- On all Junos and Junos OS Evolved platforms, the TI-LFA and Legacy LFA are mutually exclusive, and the commit check will fail and blocks LFA on one instance. PR1704521
- The BGP sessions will flap after the RE switchover. PR1705938
- 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
- Stale entries present in the lsdist table after ISO address change. PR1713008
- Multipath route is not getting compute and skip the multipath eligibility check. PR1716153
- BGP connection doesn't establish when it is configured with rfc8950-compliant under logical-systems on all Junos and Junos OS Evolved platforms. PR1716946

- Unexpected behavior of bandwidth based metric for IS-IS protocol. PR1718734
- The rpd process crashes when TI-LFA is enabled.PR1719033
- BGP multipath calculation or recalculation causes the rpd to crash. PR1719498
- RPD process crashes on all Junos and Junos OS Evolved platforms after adding static route to the VRF in some scenarios. PR1720240
- Slow convergence of PIM joins causes temporary traffic loss with scaled downstream interfaces. PR1720708
- Packet loss observed when Junos Evolved PTX platforms with Graceful Restart enabled have rpd restarted. PR1721008
- Unnecessary SPF calculation is causing high CPU utilization. PR1725686
- Multiple flaps of the interface will cause the BFD session to be down. PR1725971
- The rpd process crashes when BGP is cleaned up. PR1728455
- Traffic impact is seen when there is a single peer in the proxy BGP group connected to the BGP route reflector. PR1728604
- 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 would core rpd. PR1732833
- 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
- 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
- The rpd process crashes when routing-instance and interface is flapped repeatedly in OSPF. PR1741480
- 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 virtual router without L3VPN configuration, default MPLS table is being created unexpectedly. PR1742513
- CPU in rpd spikes and scheduler slips will be observed when the duplicate community is added. PR1745073
- 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
- No IS-IS routes being exported to the RIB, although the ISIS adjacencies are established. PR1749850
- 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

Services Applications

- A stale nat-long-route entry is present in the device causing incoming packets to be dropped. PR1719216
- L2TP tunnels may time out if creation of bbe-smgd core dump takes a long time. PR1720994

Subscriber Access Management

- Intermittent authd crash will be seen on Junos platforms in a DHCP subscriber scenario. PR1697447

- IPv4 and IPv6 address allocation will be impacted due to changes in address pool configuration. PR1715490
- Subscriber sessions will fail to login post GRES and scaled subscriber scenario. PR1723183
- Potential memory leak in authd process. PR1729035

User Interface and Configuration

- Device boots up even with incompatible configuration. PR1730442
- After device reboot BGP sessions are not coming up. PR1726731

VPNs

- The tunnel went down because the IKE exchange failed. PR1690921
- The rpd crash happens when Multicast VPN (Virtual Private Network) is configured with separate route-targets scenario. PR1700345
- MVPN tunnel is not synced to backup router. PR1710323
- The iked process will crash when VPN tunnels parameters are not matching. PR1716092

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.

NOTE: Junos OS Release 22.4 is the last-supported release for the following SKUs:

- MS-MPC-128G-BB
- MS-MPC-128G-R
- MS-MPC-128G-SX
- MS-MIC-16G
- MS-MIC-16G-SX
- SCG-TM-BAS

We recommend upgrading to MX-SPC3 **only** for the following SKUS:

- MS-MPC-128G-BB
- MS-MPC-128G-R
- MS-MPC-128G-SX

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

Basic Procedure for Upgrading to Release 22.4R3

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.

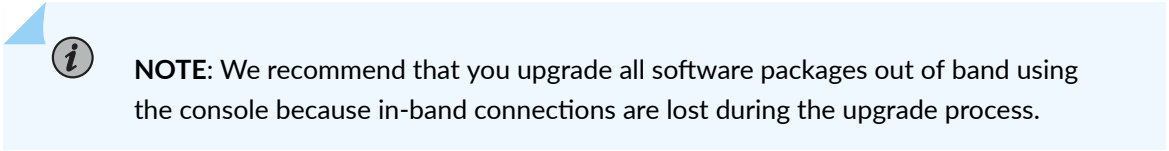
Procedure to Upgrade to Junos OS

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-x86-32-22.4R3.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-22.4R3.9-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-x86-32-22.4R3.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-22.4R3.9-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 22.4R3, 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 22.4R3

To downgrade from Release 22.4R3 to another supported release, follow the procedure for upgrading, but replace the 22.4R3 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 thirty six months after the first general availability date and customer support for an additional six more 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)	36 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 Junos OS Release 22.4R2 for NFX.

What's Changed

IN THIS SECTION

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

Software Installation and Upgrade

- **Two-step Downgrade (NFX150, NFX250 NextGen, and NFX350)**—You cannot downgrade Junos OS Release 23.1R1 directly to certain releases (listed in the **Target Release** column in No Link Title). As a workaround, you can perform downgrade as a two-step activity, in which you downgrade Junos OS Release 23.1R1 first to a corresponding intermediate release (listed in No Link Title), and then to the target release.

  Table 7: Release Compatibility for Downgrading Junos OS 23.1R1 on NFX Series Devices

Target Release	Intermediate Release
Any 22.4x release earlier than 22.4R2	22.4R2
Any 22.3x release earlier than 22.3R2.	22.3R2
• Any 22.2x release earlier than 22.2R3. • Any 22.1x release or earlier releases.	22.2R3

  PR1694074

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 NFX150 devices, after loading 22.2R1.1, the fablinks go down and the cluster status displays an FL.PR1664636
- Unable to mount the USB using USB Pass Through feature on the NFX platform. /dev/da0* files are not available. PR1748225
- IPsec tunnel behind NAT stops passing traffic when the NAT port number or IP address changes. PR1776216

High Availability

- On an NFX350 chassis cluster, when FPC0 (when node0 is primary) or FPC7 (when node1 is primary) is restarted by either using the `request chassis fpc slot slot restart node local` command or due to dcpfe core files on the primary, it restarts FPC1 or FPC8. This might break the preexisting TCP sessions and fail to restart the TCP sessions. The TCP sessions might require a manual restart. PR1557607

Interfaces

- On the NFX250, the LACP subsystem does not start automatically when the dc-pfe process is restarted.

  Workaround—Deactivate and then activate the aggregated Ethernet interface.

PR1583054

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
- On NFX250 platforms, IKED fails to install when you execute the command `request vmhost software add optional junos-ike.tgz` PR1718048

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.

Flow-Based and Packet-Based Processing

- High latency and packet drops will be observed with the `transmit-rate exact` knob enabled for one or more schedulers of an IFL/IFD.

  PR1692559

Interfaces

- On the NFX350 device, even though the ethernet cable is physically plugged in and the `show interface` command displays the Front panel LED status as `up`, the front panel LED is not ON

  PR1702799

- When issuing request support information, there was a syntax error when looking at the nfx-back-plane (was nfx-backplane, instead of nfx-back-plane)

  PR1720228

- 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 is confined to the group of ports on which the port is disabled and the other group is not affected.

  PR1731242

VPNs

- IPSec tunnel is down if IKE external-interface is configured with IPv4 and IPv6 address. As a workaround, specify the local-address inside the ike gateway object if the configured external-interface contains both IPv4 and IPv6 address hosted on it.

  PR1716697

VNFs

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

  PR1756270

- 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

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.

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 thirty six months after the first general availability date and customer support for an additional six more 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)	36 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 PTX Series

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for the PTX Series.

Class of Service

- **Enhanced host path traffic management for DDoS protection and CoS scheduling (PTX Series and QFX Series)**—Enhanced host path traffic management offers improved distributed denial-of-service (DDoS) protection and class of service (CoS) scheduling for traffic directed towards the host CPU. Using the enhanced DDoS and CoS you can:

  - Prioritize the control traffic to prevent congestion on the host interface
  - Reshape bandwidth to evenly distribute the traffic and prevent host CPU overload
  - Implement queue-specific policing to ensure traffic fairness across multiple protocols sharing the same queue and prevent undesired effects due to excessive traffic.

  These enhancements result in more stable protocol operations and bolstered system security.

  [See Understanding Class of Service and Control Plane Distributed Denial-of-Service (DDoS) Protection Overview.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for the PTX Series.

EVPN

- **Specify the UDP source port in a ping overlay or traceroute overlay operation**—In Junos OS releases prior to 22.4R1, you could not configure the udp source port in a ping overlay or traceroute overlay operation. You may now configure this value in an EVPN-VXLAN environment using `hash`. The configuration option `hash`will override any other hash-* options that may be used to determine the source port value.

General Routing

- **Single source of data for operational state sensor leaves (PTX10008)**—You can use the suppress-interface-leaf CLI statement to suppress telemetry streaming of the following sensors from the packet forwarding engine (PFE):

```
/interfaces/interface/state/high-speed
 /interfaces/interface/state/oper-status
```

  This might be required for collectors that require a single source of data for each sensor.
  [See suppress-interface-leaf.]

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.

Network Management and Monitoring

- **Changes to the NETCONF server's <rpc-error> element when the operation="delete" operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the <rpc-error> response that the NETCONF server returns when the <edit-config> operation uses operation="delete" to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the <rpc-error> element includes the <error-tag>data-missing</error-tag> and <error-type>application</error-type> elements.

- **Changes to the RPC response for <validate> operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the rfc-compliant statement at the [edit system services netconf] hierarchy level, the NETCONF server emits only an <ok/> or <rpc-error> element in response to <validate> operations. In earlier releases, the RPC reply also includes the <commit-results> element.

Platform and Infrastructure

- **The ping host | display xml command produces CLI output without errors (ACX Series, PTX Series, and QFX Series)** — In Junos OS release 22.4R2, the ping host | display xml command now produces CLI output formatted in XML.

  [See ping.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for the PTX Series.

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 all Junos OS platforms, agentd process crash will be seen in telemetry streaming longevity test. PR1647568
- On PTX10002, all odd ports have a WAN re-timer connected to it , which might introduce more time during fault recovery, such as LocalFault clear. Therefore, sometimes even if the fault is of the order of milliseconds, the port might still get hold-time expired and flap when the configured `hold-time down` less than 3s. The behavior is confirmed as hardware limitation.PR1687092
- P2MP RSVP Phase 2 MTS : Per Packet Load Balancing is not working as expected in VPTX 5000. PR1712824

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. https://kb.juniper.net/TSB18251PR1568757

Routing Protocols

- The rpd process crashes and generates a core file if 100 transport-classes are configured. PR1648490

Open Issues

IN THIS SECTION

Learn about open issues in this release for the PTX Series.

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 class-of-service (COS) commit validation is missing for classifier when using code-point-aliases. The user can configure duplicate code-point-aliases and use them in a classifier. This will result in the cosd crash. The system can be recovered by correcting the config and applying the "restart class-of-service" command.PR1766873

General Routing

- In the platform using indirect next hop (INH), such as unilist as route next hop type for multiple paths scenario (such as BGP PIC or ECMP), the session fast-reroute might be enabled in Packet Forwarding Engines. When the version-id of session-id of INH is above 256, the Packet Forwarding Engine might not respond to session update, which might cause the session-id permanently to be stuck with the weight of 65535 in Packet Forwarding Engine. It might lead Packet Forwarding Engine to have a different view of unilist against load-balance selectors. Then, either the BGP PIC or the ECMP-FRR might not work properly and traffic might be dropped or silently discarded. PR1501817
- When subscribing to sensor paths **/junos/system/linecard/packet/usage/**, **/junos/services/label-switched-path/usage/** or other line card (Packet Forwarding Engines) 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
- In Chassisd, Junos Telemetry interface thread takes more time in streaming Junos Telemetry interface packets because of the volume of data and number of sensors involved with this daemon. Junos

Telemetry interface thread engaged for more time to process streaming events cause chassisd master thread to lose receive or send keepalive messages to and from other Routing Engine, which eventually cause automatic Routing Engine switchover in most of the cases. PR1706300

- On QFX10000 and PTX Series platforms, traffic going over unilist is dropped when unilist member goes from next-hop hold state to unicast and aggregate state.PR1713279
- When system comes up with BULK Layer 2 configuration, a subsequent CONFIG delete in a way that L2ALD is still not finished processing the config create, could lead to a race condition where FLOOD ROUTE DEL event can cause l2ald crash.PR1742613
- On all Junos OS platforms, due to timing issues the PFE or PICs will be slow and services will face slowness issue and error message: 'Minor potential slow peers are: X' will be seen. This is rare timing issue.PR1747077
- On Junos OS PTX Series platforms, with Protocol Independent Multicast- Bidirectional (PIM BIDR) mode with `set protocols pim rp bidirectional` *`address group-ranges`* configuration, PIM/MLD joins will not be learnt for multicast IPs other than link local IP and MY IP which will lead to traffic impact. Also, lo0 filter which were introduced with PR 1701756 for IGMP and MLD will be applied only for MY IPs and Link local IPs. For any other IPs other than above, lo0 filter will not work.PR1774562
- On QFX10002-60c express based Junos platform the error logs are seen during boot time. These errors are not impacting any functionality. The table is getting programmed correctly. These are seen during system reboot and fpc reboot time. We will be emitting the logs for non default routing instances and not for default routing instance. PR1779890

Multicast

- On Junos OS PTX Series platforms, the traffic might silently drop or discard. This is because of the next-hop installation failure for multicast Resource Reservation Protocol (RSVP) Point to Multipoint (P2MP) traffic. This issue might only be encountered in a scaled RSVP P2MP environment after a network event which might cause reconvergence. PR1653920
- On vPTX platforms, the PFE receives an invalid token from RPD for composites next-hops due to which the PFE will crash leading to traffic drop.PR1740390

Network Management and Monitoring

- If there is management-instance configuration, it is mandatory to add "routing-instance-access".PR1766854

Routing Policy and Firewall Filters

- On all Junos OS and Junos OS Evolved platforms, the static routes are installed in the routing table even though the corresponding interface routes are not present.PR1714163

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for PTX Series.

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)

- Change in the cosd behaviour due to the CoS interface specific wildcards. PR1760817

General Routing

- Continuous error logs and Telemetry data might not be populated. PR1661423
- Currently no alarm is raised when onchip memory exhausts on paradise based FPCs. PR1690289
- Traffic loss can be seen while switching between primary and fallback sessions in MACsec setup. PR1698687

- gNMI line card (PFE) sensor /junos/system/linecard/packet/usage/ may have packet drops (gNMI translator lookup failures). PR1711779
- Next-hop programming issue at PFE on Junos PTX Series and QFX10000 platforms when the member of unilist is in hold state. PR1713279
- Received flow-routes on PTX Series routers which aren't installed as the hardware doesn't support them, lead to an FPC heap memory leak (CVE-2023-22392). PR1716398
- Traffic loop is seen due to incorrect root bridge ID. PR1717267
- Removing a PEM that doesn't have power feed does not generate the SNMP TRAP for "Power Supply Removed". PR1719915
- Convergence delay is seen when FPC is offlined under heavy traffic and scaled scenario. PR1719956
- The error logs "fpc0 expr_hostbound_packet_handler: Receive pe 254?" might be generated. PR1725716
- Upgrading the i40e NVM Firmware on Routing Engines with VM Host Support. PR1726775
- FPC crashes when the firewall filter is configured with above 65k prefixes in a single filter. PR1727067
- FPC crash observed when the ASIC usage is high. PR1727427
- Speed configuration mismatch causes the ukern core on Junos OS PTX10008 and PTX10016 platforms. PR1734703
- Junos OS: jkdsd crash due to multiple telemetry requests (CVE-2023-44188). PR1734718
- 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
- Traffic drops when next-hop installation fails in a high-scale multicast or unicast scenario. PR1738541
- Page allocation and next-hop installation failures on Junos OS PTX Series and QFX Series. PR1740190
- SPMB process will crash and PICs will not come online. PR1742186
- The rpd core files is oberved 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 memory consumption increases due to memory leak. PR1747992
- The FPC will crash on Junos PTX platforms in a rare timing issue. PR1761579

High Availability (HA) and Resiliency

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

MPLS

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

Routing Protocols

- Traffic loss is more than expected when ECMP FRR is enabled in link down scenario. PR1687887
- The mscnoopd process crash will be observed when snooping configuration is removed. PR1696374
- BGP scheduler slips during sub-optimal prefix-walk while deleting selected prefixes from a large set. PR1696870
- The rpd process might crash when SPF is recalculated. PR1699076
- Unexpected behavior of bandwidth based metric for IS-IS protocol. PR1718734
- Unnecessary SPF calculation is causing high CPU utilization. PR1725686
- The rpd process crash will be observed with BMP and independent resolution is enabled for secondary BGP routes. PR1732493
- Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute (CVE-2023-0026). PR1739919

- You can observe traffic loss in SR-LDP stitch scenario when ECMP is enabled on the PTX Series platforms. PR1746349
- No IS-IS routes being exported to the RIB, although the ISIS adjacencies are established. PR1749850
- Traffic drop is seen if chained-composite-next-hop is turned on for Segment Routing. PR1752551
- BMP leads to prolonged high rpd CPU utilization upon committing the BGP peer import policy configuration PR1729733

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 PTX Series. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

NOTE: Junos OS 22.4 is the last supported release on many PTX Series products. For more information on EOL dates, see : PTX Series Hardware Dates & Milestones.

Basic Procedure for Upgrading to Release 22.4

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: Back up the file system and the currently active Junos OS configuration before upgrading Junos OS. This allows you to recover to a known, stable environment if the upgrade is unsuccessful. Issue the following command:

```
user@host>request system snapshot
```

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 router, 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.

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 22.4R1:

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

   https://support.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 by 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 routing platform or to your internal software distribution site.

10. Install the new jinstall package on the router.

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:

```
user@host> request system software add validate reboot source/junos-install-ptx-
x86-64-22.4R1.9.tgz
```

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

```
user@host> request system software add validate reboot source/junos-install-ptx-
x86-64-22.4R1.9-limited.tgz
```

Replace the 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*

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

Adding the `reboot` command reboots 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-PTX-X8 Routing Engine. For upgrading the host OS on this

router 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.

NOTE: After you install a Junos OS Release 22.4 jinstall package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the jinstall package that corresponds to the previously installed software.

NOTE: Most of the existing `request system` commands are not supported on routers with RE-PTX-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 a Junos OS installation on each Routing Engine separately to avoid disrupting network operation as follows:

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.

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 thirty six months after the first general availability date and customer support for an additional six more 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 9: 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)	36 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

IN THIS SECTION

Learn about new features introduced in this release for QFX Series switches.

Class of Service

- **Enhanced host path traffic management for DDoS protection and CoS scheduling (PTX Series and QFX Series)**—Enhanced host path traffic management offers improved distributed denial-of-service (DDoS) protection and class of service (CoS) scheduling for traffic directed towards the host CPU. Using the enhanced DDoS and CoS you can:

  - Prioritize the control traffic to prevent congestion on the host interface
  - Reshape bandwidth to evenly distribute the traffic and prevent host CPU overload
  - Implement queue-specific policing to ensure traffic fairness across multiple protocols sharing the same queue and prevent undesired effects due to excessive traffic.

  These enhancements result in more stable protocol operations and bolstered system security.

  [See Understanding Class of Service and Control Plane Distributed Denial-of-Service (DDoS) Protection Overview.]

What's Changed

IN THIS SECTION

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

EVPN

- **Commit error if interconnect and local route distinguishers have the same value**—On EVPN data center interconnect (DCI) gateway devices, if you configure an interconnect RD at the [`edit routing-instances` *`name`* `protocols evpn interconnect`] hierarchy, the interconnect RD must be different from the local RD in the routing instance. If you try to configure the same value for the interconnect RD and the local RD in a routing instance, the device enforces this requirement by throwing a commit error. However, with DCI seamless stitching for EVPN Type 5 routes, you don't see the commit error prior to this release. Starting in this release, the device throws the commit error to enforce this condition for DCI stitching with Type 5 routes.

  [See route-distinguisher.]

General Routing

- **Autonegotiation status in show interfaces extensive output (QFX5120-48Y):**—The `show interfaces extensive` output shows the autonegotiation information for SFP-T transceivers.

- Two new alarms are added and can be seen with MPC11E when 400G-ZR optics are used. High Power Optics Too Warm: warning of the increase in chassis ambient temperature with no functional action taken on the optics Temperature too high for optics power on: New inserted optics when the chassis ambient temperature is elevated beyond the threshold will not be powered on and would need to be reinserted when the ambient temperature is within the acceptable range

- The packet rate and byte rate fields for LSP sensors on AFT (with the legacy path) have been renamed as jnx-packet-rate and jnx-byte-rate and is in parity with the UKERN behavior. Previously, these rate fields were named as packetRate and byteRate.

- 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.

- **Autonegotiation status in show interfaces extensive output (QFX5120-48Y)**—The `show interfaces extensive` output shows the autonegotiation information for SFP-T transceivers.

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).]

- **Ability to restart restart daemonized applications**—Use the `request extension-service restart-daemonize-app` *`application-name`* command to restart a daemonized application running on a Junos device. Restarting the application can assist you with debugging and troubleshooting.

  [See request extension-service restart-daemonize-app.]

Network Management and Monitoring

- **Changes to the NETCONF server's `<rpc-error>` element when the `operation="delete"` operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the `<rpc-error>` response that the NETCONF server returns when the `<edit-config>` operation uses `operation="delete"` to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the `<rpc-error>` element includes the `<error-tag>data-missing</error-tag>` and `<error-type>application</error-type>` elements.

- **Changes to the RPC response for `<validate>` operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server emits only an `<ok/>` or `<rpc-error>` element in response to `<validate>` operations. In earlier releases, the RPC reply also includes the `<commit-results>` element.

Platform and Infrastructure

- **The `ping host | display xml` command produces CLI output without errors (ACX Series, PTX Series, and QFX Series)**— In Junos OS release 22.4R2, the `ping host | display xml` command now produces CLI output formatted in XML.

  [See ping.]

- 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.]

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.

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and later, validation and upgrade might fail. The upgrade requires using the `no-validate` option to complete successfully. https://kb.juniper.net/TSB18251. PR1568757

Platform and Infrastructure

- The QFX5000 platforms can support DF only at port level granularity (In other words, for all evpn instances hosted on an ESI, only one of the Multihomed QFX5000 nodes can be DF). Below config options are recommended Have df-granularity knob (with which QFX5000 platforms seem to have

been qualified). Here, few bytes from esi value itself, instead of vlan-id are used for MOD-based DF. Another approach would be to use preference based DF election. PR1672383

- On QFX10008 devices, statistics for multicast packets is not as expected as the packets has L2 header stripped during replication in PFE because of which it is not forwarded to the next hop. PR1678723
- Dot1x daemon read the config whenever there is change in time based license for the feature MACsec.PR1713881
- The QFX10000 devices might use udp port 67 as the source port in the VXLAN udp header. PR1727072

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.

Infrastructure

- NTP time drift on the affected Junos releases. Earlier implementation of kvmclock with vDSO (virtual Dynamic Shared Object) which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate. PR1691036

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 platforms, if a speed mismatch happens in the LAG (Link Aggregation) and member interface then a traffic drop will be seen. PR1725168

Layer 2 Features

- In case of the access-side interfaces used as SP-style interfaces, when a new logical interface is added and if there is already a logical interface on the physical interface, there is 20 to 50 minutes traffic drop on the existing logical interface. PR1367488

Layer 2 Ethernet Services

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

Platform and Infrastructure

- On the QFX5100 line of switches, inserting or removing optics on a port might cause a Packet Forwarding Engine Manager CPU spike and an eventual microcode failure. PR1372041
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- In the platform using INH (indirect next hop, such as Unilist) as route next hop type for multiple paths scenario (such as BGP PIC or ECMP), the session fast-reroute might be enabled in Packet Forwarding Engines (PFEs). When the version-id of session-id of INH is above 256, the PFE might not respond to session update, which might cause the session-id permanently to be stuck with the weight of 65535 in PFE. It might lead PFE to have a different view of Unilist against load-balance selectors. Then

either the BGP PIC or the ECMP-FRR might not work properly and traffic might be dropped or silently discarded. PR1501817

- When launching a guest Virtual Machine (VM) to run a third party application on Junos OS 15.1R1 and above, the guest VM might be shown as "UNAVAILABLE" even after successfully installing the third party application. This is due to duplicated device ID assigned to different disks. PR1529596
- On QFX5110 VC, FPC may gets disconnected with 24K DHCPv6 relay scaling, after the traffic is stopped. The `pfe_listener_disconnect` error messages might get generated. PR1594748
- Pim VXLAN does not work on the TD3 chipsets enabling VXLAN flexflow after the Junos OS Release 21.3R1. Customers Pim VXLAN or data plane VXLAN can use Junos OS Release 21.3R1. PR1597276
- On all devices running Junos OS or Junos OS Evolved, where this is a high BGP scale with flapping route and the BGP Monitoring Protocol (BMP) collector/station is very slow, the rpd process might crash due to memory pressure. PR1635143
- When MACSEC and VRRP are enabled on QFX5120 VC, MACSEC sessions are flapping at random times. Without VRRP this issue is not seen. PR1640031
- On all QFX5100 Virtual Chassis platforms, after the reboot, Virtual Chassis port (VCP) ports may not establish a VCP connection and Cyclic Redundancy Check (CRC) errors are also observed. PR1646561
- On QFX platform, v6 ifl stats are being derived from the underlying ifd stats unlike on PTX where they are hardware assisted. Hence, they are not very reliable and are at best, guesstimate. PR1653671
- 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 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
- 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 RE. Work-around:- To make is master 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` command indicates duplicate entries for PSU and FAN tray after USB clean install or zeroize. PR1704106
- On Junos 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 flaps. PR1711860
- On EX4650 and QFX5120-Y devices, the 10G interfaces are not coming up simultaneously when different Small Form-factor Pluggable(SFPs - 10G and 1G) are plugged in within the same 4 port group. 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
- This problem is seen on QFX10000 platform, when ingress Sflow is enabled on bridged AE (tagged) interfaces and that incoming traffic gets forwarded via IRB interfaces on an ECMP path. In ECMP scenario, Sflow injects TAL request into the ASIC which are resulting in the traps tracked via this PR. Hence the forwarding traffic is unaffected. PR1729316
- This problem is seen on QFX10k platform, when egress Sflow is enabled on bridged AE (tagged) interfaces. In this case traffic gets forwarded via IRB interfaces to bridged AE (tagged) interfaces and to ECMP path. In case of ECMP, Sflow injects TAL request into ASIC which are resulting in the traps tracked via this PR. Original forwarding traffic is unaffected due to this problem. PR1730882
- The QFX10000 devices forwards a packet to a remote Vtep in MAC VRF even though no matching VLAN ID is found on the source port. PR1735961
- On all Junos based QFX platforms, when sflow is enabled with ECMP, ddos-protection violation of protocol group resolve is triggered. Sampled packets will be dropped and sflow will stop sending packets to the collector. This is a non-service impacting issue, however sflow will be impacted. PR1741461

Virtual Chassis

- On Junos 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

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.

EVPN

- L2ALD core at l2ald_vxlan_ifl_create_msg_build. PR1718534
- The rpd core is seen in the long-running devices with EVPN enabled. PR1723832
- Traffic loss is seen as Type 2 routes are not pushed even after withdrawing Type 5 routes. PR1723968
- 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

Layer 2 Ethernet Services

- DHCP binding is not happening in EVPN VXLAN topology with DHCP stateless relay (forward-only). PR1722082

MPLS

- The rpd process crashes during Routing Engine switchover or Route Convergence. PR1747365

Platform and Infrastructure

- The vmcore crash observed in low memory conditions. PR1694463
- The CoS rewrite rules will not be working in the EVPN with IRB scenario. PR1736890
- JUNOS:JDI_FT_REGRESSION:PROTOCOLS:SWITCHING: INTERFACE : QFX10008:: while verifying em0 statistics interface Speed is displaying in Gbps instead of mbps. PR1589942
- 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 l2circuit configurations are deleted and added back on QFX5000. PR1666260
- The QFX10000 series platforms generates error messages constantly and IPv6 routing is not performed when configured rpf-check and inet6 on VXLAN enabled interface and trying to resolve arp ndp. PR1677422
- DHCPv6 packets are not forwarded if it contains the trailer or extra bytes out of the IP stack. PR1688316
- Traffic loss is observed in IP fabric when there is a change in the underlay network. PR1688323
- The `show pfe vxlan nh-usage` command output displays incorrect overlay NH entries. PR1692596
- The interface physical link is not coming up after performing interfaces flapping on the QFX5120 device after starting traffic. PR1698228
- Minor packet drops due to hardware programming issues. PR1700927

- Power supplies in the output `show chassis environment` command displays as present state where atleast one is expected to be in OK state. PR1701240
- High CPU utilization causes a latency/slowness issue on QFX platforms. PR1704489
- Tracking PR to add the null check for list_get_head if magic is NULL. PR1705853
- The FPC crash can be seen on QFX5000 platforms during simultaneous soft and hard OIR of SFP. PR1707094
- License expire error will be observed after upgrade. PR1708794
- BFD sessions flap on EX and QFX platforms. PR1709664
- VC members are split when removing and inserting em0 cable. PR1709938
- No alarm is raised when PSU is inserted with different airflow directions. PR1710952
- When a 100G transceiver is used as a VC port or network port, the VC port or network port will either not come up or come up as 40G. PR1711407
- DHCPv6 packets could not be forwarded if it contains the trailer or extra bytes out of the IP stack. PR1711525
- The dcpfe process crash is seen on QFX5k platforms due to stale vtep entry. PR1712175
- QSFP-100G-LR4-T2 optics will stay down after ISSU/TISSU. PR1713010
- Next-hop programming issue at PFE on Junos PTX and QFX10k platforms when the member of unilist is in hold state. PR1713279
- The member interface will not be added to the AE bundle if the link-speed of the AE interface doesn't match that of the member. PR1713699
- JUNOS_REG[MACSEC]:QFX5120-48YM::dot1x-protocol subsystem is not responding to managements request verifying show security mka sessions. PR1713881
- Traffic blackhole after reboot. PR1714701
- Known multicast traffic is not forwarded when MLD snooping is enabled. PR1715429
- Untagged packets get dropped while adding a layer 3 logical unit to an interface with native vlan configured. PR1715477
- IGMP/MLD queries may get dropped if received on a port on the backup VC member when IGMP/MLD snooping is enabled. PR1716902
- The dcpfe process crashes on QFX5000 devices. PR1716996

- SNMP MIB OID output showing wrong temperature value if device running under negative temperature. PR1717105
- Traffic loop is seen due to incorrect root bridge ID. PR1717267
- Traffic egressing over the EVPN-VXLAN tunnel will drop which has AE interface as underlay. PR1718528
- Layer 2 Multicast traffic drops when PIM is configured without IGMP Snooping enabled. PR1720527
- FPC crash on QFX5120-48Y devices. PR1721297
- The dcpfe process crash will be seen on the system. PR1721316
- Error message is generated when DHCP packet is received via remote VTEP. PR1721318
- [evpn_vxlan][dcf10] More than expected traffic loss is seen when fast re-route is enabled and one of MH interfaces is bring down. PR1722348
- Unable to commit configs interface-mac-limit on sub-interfaces with vlan-tagging / flexible-vlan-tagging. PR1723400
- QFX10K not bridging multicast traffic with TTL=1 on same VLAN. PR1723433
- PFE crash is seen on Junos when file-logging is disabled. PR1723465
- 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
- On QFX5K platforms, the status of 'ECMP Resilient Hashing' will not be displayed in output of the `show forwarding-options enhanced-hash-key` command. PR1725916
- 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
- The EVPN-VXLAN proxy-arp will respond with the wrong MAC when no-mac-learning gets 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
- dcpfe process core observed after restarting the l2-learning process with flex-hashing configuration. PR1729101
- Packets received on a port that is in the `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
- Traffic for VLAN-id 2 gets dropped in Ethernet-CCC L2 Circuit on QFX5000 platforms. PR1731291
- Traffic drops when any of the VXLAN VLAN is deleted. PR1731583
- 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" knob 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 and EX platforms. PR1736348
- Unexpected VLAN tagging behavior would be observed in the EVPN-VXLAN scenario. PR1736954
- Link down due to FEC mismatch on EX4650, EX4400 and Junos based QFX5000 platforms using 25G-LR optics. PR1738077
- Blackholing of l3-inject traffic on QFX10000 platforms. PR1738197
- Traffic drop observed when encapsulation ethernet-bridge is configured on the aggregated Ethernet interface associated with VXLAN VLAN. PR1738205
- High convergence time in the EVPN-VxLAN uplink failover scenario. PR1738276
- An rpd crash will be observed due to inconsistency between rpd and kernel. PR1738820
- DSCP classifier is not created on IP interfaces. PR1738981
- On QFX5120-48Y devices, 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
- 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
- Traffic drop will be observed after extended-vni-list configuration change with EVPN-VXLAN scenario. PR1742763
- 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
- The QFX5000 devices ,when RSI (request support information) gets executed in the VC configuration, some errors output. PR1746788
- 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
- Traffic drop will be observed when Label MPLS traffic egressing out on the IRB interface as IPV4. PR1748500

Routing Policy and Firewall Filters

- Issue in committing more than 23, 4-byte AS on Junos and Junos Evolved platforms. PR1706143
- 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
- Unexpected behavior of bandwidth based metric for IS-IS protocol. PR1718734

- BGP multipath calculation or recalculation causes the rpd to crash. PR1719498
- RPD process crashes on all Junos and Junos OS Evolved platforms after adding static route to the VRF in some scenarios. PR1720240
- Multiple flaps of the interface will cause the BFD session to be down PR1725971
- 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

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 **20.3** 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-x86-64-22.4-R2.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-x86-64-22.4R2.9.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-x86-64-22.4R2.9.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 18.3R2.

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-x86-64-20.4R2.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-x86-64-20.4R2.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-
x86-64-22.4R2.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-
x86-64-22.4R2.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:

- No Link Title
- No Link Title

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-x86-64-22.4R2.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-x86-64-18.3R2.n-secure-signed.tgz ...
     Install jinstall-host-qfx-5-f-x86-64-19.2R2.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 thirty six months after the first general availability date and customer support for an additional six more 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 10: 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)	36 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

IN THIS SECTION

Learn about new features introduced in this release for SRX Series devices.

Network Address Translation (NAT)

- **Source NAT port overload (cSRX, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 22.4R1, We've updated the hash algorithm to allow for improved distribution of network traffic, when using the port overloading capability. Enabling better utilization per IP, as appropriate to the type of network traffic.

  The hash algorithm uses the reverse traffic from the server, matches the existing sessions, and reuses the same Network Address Translation (NAT) resources.

  You can configure the updated hash algorithm using the `enhanced-port-overloading-algorithm` statement at the [`security nat source pool` *`pool-name`* `port`] and [`security nat source interface`] hierarchy levels.

  [See pool (Security Source NAT) and source (Security Source NAT).]

- **Source NAT preserve range support (SRX Series)**—Starting in Junos OS Release 22.4R1, we support a preserve range for the source NAT. You can assign a port within the same range as the incoming port, either 0 through 1023 or 1024 through 65,535.

  To enable the preserve range, configure the `preserve-range` statement at the [`security nat source pool` *`pool-name`* `port`] hierarchy level.

  [See pool (Security Source NAT) and preserve-range.]

- **Support for NAT64 router advertisement (MX Series)**—Starting in Junos OS Release 22.4R1, we support NAT64 IPv6 address prefix router advertisement.

  The router advertises the configured NAT64 IPv6 address prefix in the router advertisement packets. You can configure up to three NAT64 IPv6 address prefixes per interface.

  You can configure the NAT64 IPv6 address prefix using the `set protocols router-advertisement interface` *`<interface-name>`* `nat-prefix` *`<prefix>`* command.

  You can configure the router advertisement time using the `set protocols router-advertisement interface` *`<interface-name>`* `nat-prefix` *`<prefix>`* `lifetime` *`<lifetime>`* command.

[See IPv6 Neighbor Discovery, interface (Protocols IPv6 Neighbor Discovery), and show ipv6 router-advertisement.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series.

Network Management and Monitoring

- **Changes to the NETCONF server's <rpc-error> element when the operation="delete" operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the <rpc-error> response that the NETCONF server returns when the <edit-config> operation uses operation="delete" to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the <rpc-error> element includes the <error-tag>data-missing</error-tag> and <error-type>application</error-type> elements.

- **Changes to the RPC response for <validate> operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the rfc-compliant statement at the [edit system services netconf] hierarchy level, the NETCONF server emits only an <ok/> or <rpc-error> element in response to <validate> operations. In earlier releases, the RPC reply also includes the <commit-results> element.

Routing Policy and Firewall Filters

- **Syslogs to capture commit warning messages related to traffic loss prevention over VPN (SRX, vSRX, NFX platforms)**—Configuration commit warnings such as warning: Policy 'traditional' does not contain

`any dynamic-applications or url-categories but is placed below policies that use them. Please insert policy 'traditional' before your Unified policies` or *warning: Source address or address_set (made_up_address) not found. Please check if it is a SecProfiling Feed* caused the MGD to inform IKED or KMD process about *DAX_ITEM_DELETE_ALL* resulting in VPN flaps and outage events. These warnings messages are captured by syslogs to prevent traffic loss over VPN. We recommend you to resolve these syslog warning messages to prevent major outages.

VPNs

- **Enhancements to alternate subject name in the output of show security pki local-certificate command (SRX Series, vSRX 3.0)**—Certificate having multiple FQDN now displays all the related domains, IPv4 or IPv6 addresses and email addresses in the `Alternate subject` field. These enhancements are seen in the output of `show security pki local-certificate` command. Earlier the command output displayed only the last FQDN details.

  [See show security pki local-certificate (View).]

- **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.]

- **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.

- **Limited ECDSA Certificate Support with SSL Proxy (SRX Series and vSRX 3.0)**—With SSL proxy configured on SRX Series firewall and vSRX Virtual firewalls:

  - ECDSA based websites with P-384/P-521 server certificates are not accessible with any root-ca certificate as the security device has limitation to support only P-256 group.

  - When RSA based root-ca and P-384/P-521 ECDSA root-ca certificate is configured, all ECDSA websites will not be accessible as SSL-Terminator is negotiated with RSA, which is why the security device is sending only RSA ciphers and sigalgs to the destination web server while doing the SSL handshake. To ensure both ECDSA and RSA-based websites are accessible along with the RSA root certificate, configure a 256-bits ECDSA root certificate.

- In some scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server does not support P-256 groups.
- In other scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server supports sigalgs other than P-256. The issue is seen in hardware offload mode with failing signature verification. As hardware offload for ECDSA certificate is introduced in Junos OS release 22.1R1, this issue will not be observed if you use Junos OS released prior to 22.1R1. Also, the issue is not seen if the SSL-proxy for ECDSA certificate is handled in software.

Known Limitations

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

- 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
- On SRX380, the Autonegotiation status on the 1G/10G ports may be incorrectly displayed as "Incomplete". This has no impact to traffic. PR1703002

Network Address Translation (NAT)

- While port ranges are configured as part of NAT source pool. The port affinity allocation might fail as when the affinity allocation is failed for a flow then the port random allocation is set. The random allocation can allocate any port and the allocation failure can grow. PR1678563

Open Issues

Learn about open issues 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.

General Routing

- IPSec rekey fails when SRX is configured with kilobyte based lifetime in remote access solution. PR1527384
- With ssl-proxy configured along with web-proxy, the client session might not get closed on the device until session timeout, even though the proxy session ends gracefully.PR1580526
- Device does not drop session with server certificate chain more than 6.PR1663062
- FIPS mode is not supported in this release for SRX devices.PR1697999
- On Junos (FreeBSD) platforms, kernel panic was seen.PR1709013

Chassis Clustering

- DSCP remarking is required to classify BFD packets as high priority. PR1693457

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

Infrastructure

- NTP time drift on the affected Junos releases. Earlier implementation of kvmclock with vDSO (virtual Dynamic Shared Object) which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate.PR1691036

Layer 2 Ethernet Services

- If a client sends a DHCP request packet, and option 55 includes PAD option (0), a DHCP ACK will not be sent back to the client. PR1201413

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
- On all SRX platforms in chassis cluster which support ISSU, when the JUNOS IKE package is present and IPSec VPN is configured, ISSU is not supported from any release before 22.4R1 to 22.4R1 or

later. You can use CLI command 'show version' to confirm if JUNOS IKE package is present on your device.PR1722689

Resolved Issues

Learn about the issues fixed 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.

Application Layer Gateways (ALGs)

- The first FTPS session will not work on SRX5K platforms leading to a traffic drop PR1715918
- Device crashed while processing H323 traffic in SRX and MX PR1722877
- SIP ALG not working for SIP traffic with MIME header and traffic is dropped PR1728638

Authentication and Access Control

- Connection fails are observed on Junos despite a valid auth entry PR1692398

Chassis Clustering

- Unsupported configuration for interface st0.16000-16385 is possible when using replace pattern on SRX platforms PR1731593
- In SRX MNHA cluster setup the RSI takes long time to generate PR1736498
- BFD session fails to re-establish on SRX cluster mode PR1737520

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

- Packet loss is observed for IPSec sessions when PMI is enabled PR1692885
- The traffic will fail when accessing the routing instance interface IP from external IP PR1719437

- The IPv6 Neighbor Discovery fails on VLAN tagged reth interfaces PR1720570

General Routing

- 8-Port Gigabit Ethernet SFP XPIM not passing traffic after software upgrade PR1620982
- BGP down due to BFD expired; failover restored services PR1630981
- [SRX] SRX550HM interfaces LED of ge-0/0/6-9 will auto turn off after device bootup some minutes PR1634965
- The DNS information is getting lost when IPCP flaps PR1658968
- fxp0 works under disable state in SRX300 PR1661816
- SRX Branch models are unable to connect to domain controller on installing Microsoft KB update PR1683420
- On all Junos lsys systems RPD process crashes due to JET client invoking rpc handled by RPD daemon PR1692738
- The user-id entries will not be synced with secondary node PR1701990
- Log streaming Hosts configured as FQDN may fail when DNS re-query is performed PR1708116
- High latency will be observed while pinging to peer device PR1714620
- The firewall web-authentication feature will not work after enabling Juniper secure connect PR1714845
- Interface speed stays 100Mbps when removing speed and duplex command separately PR1715247
- The nsd process may report an error msg PR1715297
- J-flow sends wrong IP in sampling records when NAT is configured for traffic along with input sampling PR1716707
- Security log missing space between timestamp and hostname PR1716776
- The SSL session drops because of the wrong SNI value PR1716893
- Errors seen under interfaces in slot0 option PR1717095
- The srxpfe core has been seen on secondary SRX during ISSU PR1717503
- OAM not working with flexible-vlan-tagging PR1719108
- The flowd process crash is observed when the web proxy packet reinjection fails PR1719703

- Local route is not added in the secondary FIB on all Junos SRX platforms and routes will be permanently stuck in KRT queue PR1721032
- Nstraced process is running high on the primary node after the Junos upgrade PR1727122
- L2 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 DNS cache gets wiped out due to the flowd crash on all SRX platforms after the upgrade PR1732028
- nsd crash impacting remote access vpn on SRX devices PR1732746
- 23.2R1 :USF_DNSF:log messages are not generated when Sending MX query with domain name in black list with action as report after configure the web filtering with one/morep profile and template. PR1733435
- Intermittent core-dumps is received when SMB protocol is enabled on AAMW policy and PFE memory is exhausted PR1737442
- Junos OS installation using USB can fail on SRX4600 PR1737721
- Failover can be seen on SRX5K cluster with SPC2 cards while executing RSI PR1738188
- "Minor Autorecovery information needs to be saved" alarm is not displayed after zeroize PR1738271
- Traffic drop caused by PFE memory leak on SRX platforms PR1738656
- SRX4100/4200 accepts the datapath-debug configuration although it does not support it PR1739559
- Processing a TWAMP packet and terminating the TWAMP session will cause a core-dump in a corner case scenario PR1739733
- flowd process crash observed in Junos branch SRX platforms PR1743107
- Commit panic reboot observed after implementing system processes watchdog timeout 180 on SRX hardware platforms PR1744108
- One of the node in high availability/cluster will go offline briefly PR1749584
- SPC3 PIC crash PR1749830
- Users authenticated via captive portal experience a noticeable delay of atleast 2-5 mins PR1755593

Intrusion Detection and Prevention (IDP)

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

J-Web

- 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
- Cannot add custom defined security address-book under Security Policies Objects > Security Policies > Create > Source Zone > Select Sources. PR1748078

Network Address Translation (NAT)

- Some sessions will not be deleted when the NAT rule is deleted from the system PR1712738

Platform and Infrastructure

- 22.2R1:FIPSCC:L2HA:After RG0 failover, node priority are set to zero for node0 with Relinquish monitoring failure. PR1670772
- 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

- The flowd process crash is observed with the security policy updated with changing IP address related to the FQDN PR1713576
- The nsd process crash is seen when ISSU is performed on the cluster PR1724777
- Traffic impact is observed when the security policy is configured with a huge number of addresses and on addition/deletion of these policies PR1725567

Routing Protocols

- The traffic drop will be observed for the static route after VRRP failover when VRRP VIP is set as next-hop for that static route PR1687884
- 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 virtual router without L3VPN configuration, default MPLS table is being created unexpectedly PR1742513

Unified Threat Management (UTM)

- utmd core has seen at commit when *.* or *.*.* is configured at url-pattern PR1715260
- Memory leak is observed on all Junos SRX platforms with http-persist and http-reassembly configuration PR1725359
- Outlook notification channel connection is not established PR1725938

VPNs

- The tunnel went down because the IKE exchange failed PR1690921
- Cold sync status of MNHA nodes may go into an INCOMPLETE state after bootup. PR1710374
- The iked process will crash when VPN tunnels parameters are not matching PR1716092
- ISSU is aborted and flowd process crash is observed PR1722122
- 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 thirty six months after the first general availability date and customer support for an additional six more 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 11: 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)	36 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

- **Changes to the NETCONF server's `<rpc-error>` element when the `operation="delete"` operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the `<rpc-error>` response that the NETCONF server returns

when the <edit-config> operation uses operation="delete" to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the <rpc-error> element includes the <error-tag>data-missing</error-tag> and <error-type>application</error-type> elements.

- **Changes to the RPC response for <validate> operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the rfc-compliant statement at the [edit system services netconf] hierarchy level, the NETCONF server emits only an <ok/> or <rpc-error> element in response to <validate> operations. In earlier releases, the RPC reply also includes the <commit-results> element.

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

IN THIS SECTION

Learn about open issues 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

- The input fifo errors drops reported under pfe shell show ifd but not seen in show interface extensive output. PR1642426

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

- PFE syslog tags are missing for the command help syslog "^PFE_?". PR1707504

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 22.4R3, see "Known Limitations" on page 59 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

- BGP multipath calculation or recalculation causes the rpd to crash. PR1719498
- The DNS cache gets wiped out due to the flowd crash on all SRX platforms after the upgrade. PR1732028
- Constant BGP peer flaps would core rpd. 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

Learn about what changed in this release for vSRX.

Network Management and Monitoring

- **Changes to the NETCONF server's <rpc-error> element when the operation="delete" operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the <rpc-error> response that the NETCONF server returns when the <edit-config> operation uses operation="delete" to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the <rpc-error> element includes the <error-tag>data-missing</error-tag> and <error-type>application</error-type> elements.

- **Changes to the RPC response for <validate> operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the rfc-compliant statement at the [edit system services netconf] hierarchy level, the NETCONF server emits only an <ok/> or <rpc-error> element in response to <validate> operations. In earlier releases, the RPC reply also includes the <commit-results> element.

Platform and Infrastructure

- **Cloud Initialization (vSRX)**—Cloud-init is supported by vSRX 3.0 on KubeVirt with the NoCloud datasource.

  [See KubeVirt user guide.]

Routing Policy and Firewall Filters

- **Syslogs to capture commit warning messages related to traffic loss prevention over VPN (SRX, vSRX, NFX platforms)**—Configuration commit warnings such as warning: Policy 'traditional' does not contain any dynamic-applications or url-categories but is placed below policies that use them. Please insert policy 'traditional' before your Unified policies or *warning: Source address or address_set (made_up_address) not found. Please check if it is a SecProfiling Feed* caused the MGD to inform IKED or KMD process about *DAX_ITEM_DELETE_ALL* resulting in VPN flaps and outage events. These warnings messages are captured by syslogs to prevent traffic loss over VPN. We recommend you to resolve these syslog warning messages to prevent major outages.

VPNs

- **Enhancements to alternate subject name in the output of show security pki local-certificate command (SRX Series, vSRX 3.0)**—Certificate having multiple FQDN now displays all the related

domains, IPv4 or IPv6 addresses and email addresses in the `Alternate subject` field. These enhancements are seen in the output of `show security pki local-certificate` command. Earlier the command output displayed only the last FQDN details.

[See show security pki local-certificate (View).]

- **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.]

- **Limited ECDSA Certificate Support with SSL Proxy (SRX Series and vSRX 3.0)**—With SSL proxy configured on SRX Series firewall and vSRX Virtual firewalls:

  - ECDSA based websites with P-384/P-521 server certificates are not accessible with any root-ca certificate as the security device has limitation to support only P-256 group.
  - When RSA based root-ca and P-384/P-521 ECDSA root-ca certificate is configured, all ECDSA websites will not be accessible as SSL-Terminator is negotiated with RSA, which is why the security device is sending only RSA ciphers and sigalgs to the destination web server while doing the SSL handshake. To ensure both ECDSA and RSA-based websites are accessible along with the RSA root certificate, configure a 256-bits ECDSA root certificate.
  - In some scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server does not support P-256 groups.
  - In other scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server supports sigalgs other than P-256. The issue is seen in hardware offload mode with failing signature verification. As hardware offload for ECDSA certificate is introduced in Junos OS release 22.1R1, this issue will not be observed if you use Junos OS released prior to 22.1R1. Also, the issue is not seen if the SSL-proxy for ECDSA certificate is handled in software.

Known Limitations

Learn about known limitations 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.

Chassis Clustering

- Currently max BFD detection interval tested by RLI is 16s. If the detection interval is too large, no BFD down event will be posted by BFDD daemon to jsrpd and jsrpd cannot be aware that ICL once goes down since BFD is the single source of MNHA ICL link failure detection. We don't have other (or plan to add other) ways to detect ICL link going down as it introduces extra complexity. So currently this is a product-limitation.PR1671622

VPNs

- In case of IKEv2, if the IKE and IPsec SA setup fails in the IKE-SA-AUTH exchange at the initiator end(due to authentication failure), it will lead to a situation where in the responder would have already brought up the IKE and IPsec SA and there would be no delete notification sent from initiator to the responder. To avoid such a scenario, it is recommended to enable dead-peer-detection (DPD) on the responder end which will ensure that the IKE and IPsec SAs gets deleted on the responder. PR1680885

Open Issues

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.

General Routing

- With ssl-proxy configured along with web-proxy, the client session might not get closed on the device until session timeout, even though the proxy session ends gracefully. PR1580526
- Device does not drop session with server certificate chain more than 6. PR1663062
- When APBR profile is configured as a policy (and not attached to a security zone) and a failover occurs in between a long-lived ALG(FTP-DATA) session, then the APBR info won't be populated in the AppTrack session close log from the backup node. This issue will be seen only when the (FTP) control session and the ALG(FTP-DATA) session are not "Active" on the same node. PR1688021
- FIPS mode is not supported in this release for SRX devices. PR1697999

Infrastructure

- NTP time drift on the affected Junos releases. Earlier implementation of kvmclock with vDSO (virtual Dynamic Shared Object) which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate. PR1691036

VPNs

- When using Group VPN, in certain cases, the PUSH ACK message from the group member to the group key server may be lost. The group member can still send rekey requests for the TEK SAs before the hard lifetime expiry. Only if the key server sends any new PUSH messages to the group members, those updates would not be received by the group member since the key server would have removed the member from registered members list. PR1608290

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.

Chassis Clustering

- Traffic loss after RG1 failover. PR1726753

Flow-Based and Packet-Based Processing

- High latency and packet drops will be observed with the "transmit-rate exact" knob enabled for one or more schedulers of an IFL/IFD. PR1692559
- Packet loss is observed for IPSec sessions when PMI is enabled. PR1692885
- On SRX platforms, tunnel fails to come up when tunnel destination routing instance is configured. PR1693767
- Packets are dropped because flow sessions will not be created for the MPLS routed traffic. PR1703678
- The inet6 packet mode drops traffic significantly. PR1733819
- Virtual Routing Instance configured on ingress interface will drop the icmp traffic. PR1742739

General Routing

- Log streaming Hosts configured as FQDN may fail when DNS re-query is performed. PR1708116
- Security log missing space between timestamp and hostname. PR1716776
- The flowd process crash is observed when the web proxy packet reinjection fails. PR1719703
- The DNS cache gets wiped out due to the flowd crash on all SRX platforms after the upgrade. PR1732028
- Traffic drop caused by PFE memory leak on SRX platforms. PR1738656

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

Platform and Infrastructure

- When deploying a new vSRX on Azure, if "Accelerated" is selected for the initial interface selected by default, the vSRX will duplicate the fxp0 interface MAC address to ge-0/0/0 and make that interface unusable. As a workaround, de-select “Accelerated” from the interface at the initial deployment. PR1726091

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 22.4R1 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 22.4R1 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 22.4R1 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 22.4R1 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 thirty six months after the first general availability date and customer support for an additional six more 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 12: 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)	36 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.

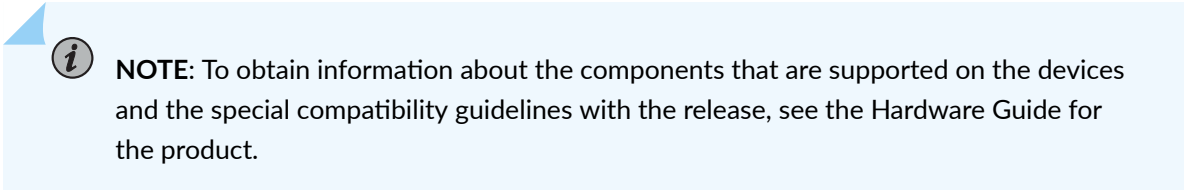
  https://apps.juniper.net/feature-explorer/

- **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



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

- **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

15 August 2025—Revision 6, Junos OS Release 22.4R3.

16 June 2025—Revision 5, Junos OS Release 22.4R3.

3 April 2025—Revision 4, Junos OS Release 22.4R3.

27 March 2025—Revision 3, Junos OS Release 22.4R3.

5 April 2024—Revision 2, Junos OS Release 22.4R3.

14 February 2024—Revision 1, Junos OS Release 22.4R3.