Release Notes

Published
2025-12-04

Junos OS Release 24.2R2®

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cPCE, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall. This release notes accompany Junos OS Release 24.2R2. 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

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cPCE, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series Firewall, and vSRX Virtual Firewall. This release notes accompany Junos OS Release 24.2R2. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

- Change to the commit process—In prior Junos OS and Junos OS Evolved releases, if you use the commit prepare command and modify the configuration before activating the configuration using the commit activate command, the prepared commit cache becomes invalid due to the interim configuration change. As a result, you cannot perform a regular commit operation using the commit command. The CLI shows an error message: 'error: Commit activation is pending, either activate or clear commit prepare'. If you now try running the commit activate command, the CLI shows an error message: 'error: Prepared commit cache invalid, failed to activate'. You then must clear the prepared configuration using the clear system commit prepared command before performing a regular commit operation. From this Junos and Junos OS Evolved release, when you modify a device configuration after 'commit prepare' and then issue a 'commit', the OS detects that the prepared cache is invalid and automatically clears the prepared cache before proceeding with regular 'commit' operation.

  [See Commit Preparation and Activation Overview.]

- In a firewall filter configured with a port-mirror-instance or port-mirror action, if l2-mirror action is also configured, then port-mirroring instance family should be any. In the absence of the l2-mirror action, port-mirroring instance family should be the firewall filter family.

- Support added for interface-group match condition for MPLS firewall filter family.

EVPN

- **EVPN system log messages for CCC interface up and down events**—Devices will now log EVPN and EVPN-VPWS interface up and down event messages for interfaces configured with circuit cross-connect (CCC) encapsulation types. You can look for error messages with message types EVPN_INTF_CCC_DOWN and EVPN_INTF_CCC_UP in the device system log file (`/var/log/syslog`).

Routing Protocols

- **Update to IGMP snooping membership command options**— The `instance` option is now visible when issuing the `show igmp snooping membership ?` command. Earlier, the `instance` option was available but not visible when `?` was issued to view all possible completions for the `show igmp snooping membership` command.

  [See show igmp snooping membership.]

- **MLD snooping proxy and l2-querier source-address (ACX7024, ACX7100-32C, EX4400-24MP, PTX10001-36MR, QFX5120-32C, and QFX5130-32CD)**— The `source-address` configured for `proxy` and `l2-querier` under the `mld-snooping` hierarchy should be an IPv6 link-local address in the range of fe80::/64. The CLI help text has been updated to "Source IPv6 link local address to use for proxy/L2 querier". In earlier releases, the CLI help text read, "Source IP address to use for proxy/L2 querier."

  [See source-address.]

User Interface and Configuration

- **The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX and vSRX)**—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the `Hostname` field first instead of last. The `show version` command output includes the `Family` field. The `Family` field identifies the device family under which the device is categorized, for example, `junos`, `junos-es`, `junos-ex`, or `junos-qfx`.

  [See show system information and show version.]

Known Limitations

IN THIS SECTION

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

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

General Routing

- The configuration to logout console session on disconnect does not work on ACX710. PR1791623
- Impacted Platform : ACX710 Feature : Ingress sflow (Sw) Issue : In sflow records, output field will be always Zero , as this cannot be supported due to HW limitation. PR1842399

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

- JDI-RCT:ACX : Syslog error @Err] dnx_rt_vswitch_cross_connect_add_del: dnx_rt_vswitch_cross_connect_add_del:cross-connect delete failed for IFL 135(UNI 1149255708,NNI 402657548) (-1:Internal. PR1732448
- On ACX1000/2000/3000 platforms, MPLS load-balancing on AE (Aggregated Ethernet) interfaces with more than one member link may not work as expected after upgrading Junos to 20.1R1 or later releases. PR1739480
- When restart chassis-control trigged on M/MX router has configuration with ccc instance, syslog is error out " Err] ACX_ASIC_PROGRAMMING_ERROR: pfe_dnx_translation_set: Error, bcm_vlan_port_translation_set rv:Entry not found ".PR1764966
- On ACX5048and ACX5096 platform, after the device is upgraded, disabling an interface and then rebooting the device will cause a critical issue. All interfaces will go down, resulting in a complete traffic drop. There is no known workaround to prevent this service interruption during the upgrade process. PR1786687
- ACX1100 PTP(enterprise profile) is stuck at freerun state after upgrading junos to 21.2R3. PR1789694
- When ACX2200 deploys l2circuit with hot-standby mode, it fails to forward the traffic after a few rounds of consecutive neighbor failover and link cutover. Standby mode does not have such problem. PR1797017
- ACX710 does not recognize GPON OLT 740-124448 reports NON-JNPR after ACX power cycle. The same error state NON-JNPR can be observed when GPON OLT SFP is installed into ACX router. PR1801112
- Multicast route is reset every 5 mins with igmp receiver on acx2200 with small traffic loss. Multicast route that are not active would get reset after 5 minutes due to cahce timeout. This was happening even for active routes that had traffic. PR1805017
- On ACX2200, when interfacing with ACX7024 port will be down if a 10-Gigabit Ethernet port is set to operate at 1G speed. It will impact the services due to interface down. PR1807801
- On ACX2200 series, ge (gigabit ethernet) interfaces configured for PTP (Precision Time Protocol), after PTP is deactivated and activated or activated for the first time, traffic can experience packet drops. PR1811850

Junos XML API and Scripting

- On all Junos platforms where snapshot is supported, when a device is rebooted from recovery mode it fails to commit configuration due to problems with slax import and device might go into amnesiac mode due commit fail. PR1717425

Network Management and Monitoring

- Issue: Multiple traps are generated for single event, when more target-addresses are configed in case of INFORM async notifications Cause: INFORM type of async notification handling requires SNMP agent running on router to send a Inform-Request to the NMS and when NMS sends back a get-response PDU, this need to be handled. In this issue state, when more than one target-address(NMS IP) is configured for a SNMP v3 INFORM set of configuration, when Get-Response comes out of order in which the Inform-Request is sent, the PDU is not handled correctly causing snmp agent to retry the Inform-request. This was shown as multiple traps at the NMS side. Work-around: For this issue would be to use 'trap' instead of 'inform' in the "set snmp v3 notify NOTIFY_NAME type inform" CLI configuration. PR1773863

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

- The KRT queue will be stuck on Junos ACX710 platform. PR1787707
- Acx-arm-feb core might be triggered if IGMP snooping is enabled and IGMP query is received on the same port as IGMP join. PR1799619
- Trace route missing intermediate hops on hosts connected to ACX710. PR1808160
- Multi-protocol label switching Experimental (MPLS EXP) bit marking not working as expected causing the traffic to be wrongly classified. PR1809169
- ACX710 PTP ports marked 'passive' instead of 'primary' during T-GM selection. PR1810429
- Label corruption is seen in l2circuit redundancy when the primary l2circuit is reachable through the backup. PR1811884
- [ACX7000 Series] DHCPv4/v6 packets might be dropped because DHCP packets are not routed to kernel after initial jdhcpd starts. PR1816246
- Traffic blackholing will be observed in the l2circuit scenario when a non-active path is shut or disabled. PR1816807
- ACX platforms running EVPN-VXLAN in DCI stitching environments will experience traffic outage. PR1817677
- The ARP packet is not sent toward the EVPN core when the route for the destination IP for Layer 3 traffic is not present. PR1817707
- Network Protocol Outage on ACX Junos platforms due to SER of Memory ECC Parity Errors. PR1823195
- The cosd process crash with major application cosd fail alarm is seen after enabling host-outbound-traffic without forwarding class. PR1825959
- ACX5448-M - SFP-T flapping issues. PR1828714
- On Junos ACX710 Platforms the clksyncd error is seen affecting IPC. PR1829340
- Configuration Archival does not work using SFTP when using the mgmt_junos routing-instance on ACX5448. PR1833705
- Packets are forwarded with native VLAN tagged on ACX5448 and ACX710 platforms. PR1849241
- Inner VLAN tag DEI bit in VLAN header set incorrectly. PR1850907
- EVPN protocol configuration through CLI is not allowed on device. PR1852905

- Esi link state change causing bum traffic block. PR1853321

Class of Service (CoS)

- Multiple adjacencies might get dropped over AE interfaces. PR1828018

Interfaces and Chassis

- The LFM session flaps will be observed at random. PR1811734

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, 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 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
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.

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.

General Routing

- **Enhancement to fix output with Junos PyEz for duplicate keys in PKI (MX Series, SRX Series, EX Series)**—In earlier releases, though the CLI output displayed all the duplicate keys for the corresponding hash algorithms in PKI using `show security pki local-certificate detail | display json` command, for the same requested data, Junos PyEz displayed the last key only. Starting this release, the CLI output and Junos PyEz displays all the duplicate keys with the enhanced tags.

Routing Protocols

- **MLD snooping proxy and l2-querier source-address (ACX7024, ACX7100-32C, EX4400-24MP, PTX10001-36MR, QFX5120-32C, and QFX5130-32CD)—** The `source-address` configured for `proxy` and `l2-querier` under the `mld-snooping` hierarchy should be an IPv6 link-local address in the range of fe80::/64. The CLI help text has been updated to "Source IPv6 link local address to use for proxy/L2 querier". In earlier releases, the CLI help text read, "Source IP address to use for proxy/L2 querier."

  [See source-address.]

User Interface and Configuration

- The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX and vSRX)—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the `Hostname` field first instead of last. The `show version` command output includes the `Family` field. The `Family` field identifies the device family under which the device is categorized, for example, `junos`, `junos-es`, `junos-ex`, or `junos-qfx`.

  [See show system information and show version.]

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.

General Routing

- On EX2300, EX3400, EX4300-48MP and EX4300 , Pause frames counters does not get incremented when pause frames are sent.PR1580560
- [interface] [all] EX4400-48F :: JUNOS_REG: EX4400 : input-vlan-tagged-frames are not in the expected range while verifying Vlan Tagged FramesPR1749391
- "Error:tvp_optics_eeprom_read: Failed to read eeprom for link" logs might be seen for some time during system reboot or pfe restart in EX3400. There is no functional impact due to these logs.PR1757034

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.

General Routing

- misleading syslog message "L2CKT/L2VPN acquiring mastership for primary" though no VPN/L2CKT configured on the routerPR1105459
- runt, fragment and jabber counters are not incrementing on EX4300-MPsPR1492605
- On all EX platforms, whenever beacon LED functionality is enabled, there is a mismatch between the physical LED status and the output of the CLI command ?show chassis led? showing incorrect port LED status for interfaces as LED up instead of off.PR1697678
- The interface of ge-x/0/1 port might go down after virtual-chassis split and merge on EX4300-VCPR1745855
- EX4300MP: VC member status toggling between "Inactive" and "NotPrsnt" state after member downgradePR1751871
- on EX2300-48 MP without VC pre-provisioned configuration, If master's member-id and master member's interface config are changed then VC is taking more time to get stabilized.PR1764542
- After rebooting a mixed Virtual Chassis (VC) of EX4300-xxP and EX4300-MP switches or rebooting a EX4300-xxP member, interfaces with Power over Ethernet (PoE) configured will not come up on EX4300-xxP members.PR1782445
- Ex-Hardening:Local/Remote fault insertion from TG is failingPR1789999
- On EX4300-MP platforms, ge (Gigabit ethernet) interfaces configured for 10 or 100Mbps (Mega bits per second), jumbo frame packets will be dropped.PR1812891
- For Junos OS platforms, in a specific configuration change after NSSU (Nonstop Software Upgrade), i.e. delete and add sequence of LAG (Link Aggregation Group) bundles performed via load baseline configuration and re-apply original configuration, OSPF (Open Shortest Path First) session might get stuck in EXSTART state. This issue will impact the traffic.PR1817034
- On Junos platforms, if disk is full, when scaling configuration is moved to baseline configuration and move back to scaling configuration, l2ald try to create a source VTEP, but old VTEP is still in the middle of deletion, so kernel return EBUSY and l2ald will retry. If retry too many times, l2ald insist and core.PR1817705

- Traffic loss will be seen on 1G-SFP-T if speed is configured to 100m. 1G SFP-T has the AN feature enabled but the PHY we have b/w SFP-T and switch ie., PHY82756 doesn't support AN and this mismatch is causing the traffic loss. This needs feature enhancement PR1817992
- Time Domain Reflectometry (TDR) support for detecting cable breaks and shorts aborts intermittently on some random ports.PR1820086
- On Junos QFX and EX platforms in an EVPN-VXLAN (Extended Virtual Private Network- Virtual Extensible LAN) CRB (Centrally-Routed Bridging) scenario where the ingress leaf switch is configured with ESI (Ethernet Segment Identifier) lags (i.e. the server is multihomed), if there is an overlap between ESI lag(s) trunk ID with physical port number(s) and overlap of DMAC (destination MAC) between VGA (Virtual Gateway Address) MAC address 00:00:5e:00:01:01 (CRB setup with VGA / GW is on spine) with VRRP (Virtual Router Redundancy Protocol) MAC (specifically for the VRRP group 1 MAC address 00:00:5e:00:01:01) on the physical ports of the Leaf switches, then traffic loss will be observed for the inter-VLAN traffic.PR1820830
- On all Junos QFX5K platforms, with ECMP (Equal Cost Multi Path) configured, when there is any routing protocol change (like ISIS cost metric change), the protocol traffic on the network is dropped.PR1823601
- On a working VC system, if there happens a dc-pfe process restart for any reasons, then there is a possibility of some interfaces not getting created after the dc-pfe restart.PR1823688
- When a poe bounce command is issued in quick succession for multiple ports, the 'poe enabled' logs may not be printed for some of the poe ports. This is a cosmetic issue and functionality works as expected.PR1845161
- For EX4100 platforms, with default UFT profile configured and high scale of IPv6 host routes, hash collisions may prevent routes from being installed in the ipv6 host table. Additionally, these routes might not get installed in the LPM table as well because the size limit for ipv6 prefix > 64 is restricted to 1k, resulting in table full errors. This can result in traffic loss. When the issue occurs, below error message could be observed: fpc0 brcm_rt_ip_uc_lpm_install:1583(LPM route change failed) Reason : Table full unit 0 fpc0 brcm_rt_ip_uc_host_install:2355(ip host add into LPM table failed) Reason :Operation failed fpc0 brcm_rt_ip_uc_entry_install:1321brcm_rt_ip_uc_entry_install Error: host(/32) ip route install failed vrf 9 ip 100:27::52:102 nh-swidx 6381 nh-hwidx 400215PR1849471

High Availability (HA) and Resiliency

- Graceful Routing Engine Switchover (GRES) not supporting the configuration of a private route, such as fxp0 , when imported into a non-default instance or logical system. Please see KB https://kb.juniper.net/InfoCenter/index?page=content=KB26616 resolution rib policy is required to apply as a work-aroundPR1754351

Platform and Infrastructure

- An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on EX4300 Series allows a locally authenticated attacker with low privileges to cause a Denial-of-Service (Dos). Please refer to https://supportportal.juniper.net/JSA79186 for more information.PR1774634
- On EX4300 or EX4300-VC, removal of a Physical Interface Card (PIC), or if the software fails to detect a PIC that is installed, it can cause a crash in the pfex process. This crash can lead to high CPU usage and potentially disrupt network traffic.PR1779410
- On EX4300 Platforms, Packet Forwarding Engine (PFE) crash will be seen due to an unexpected switchover after committing interface configuration .PR1785058
- VSTP BPDU are not properly processed by EX4300 when the interface is configured in SP style causing VSTP not to convergePR1849492

Routing Protocols

- On all Junos and Junos OS Evolved platforms, multiple simultaneous Command Line Interface (CLI) sessions will lead to high Management Daemon (mgd) CPU utilization, impacting the device's reachability over the loopback interface from IS-IS nodes.PR1749850

Resolved Issues

IN THIS SECTION

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

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

EVPN

- Error messages are observed after performing a VLAN name change with EVPN configuration PR1806660

Forwarding and Sampling

- The fxpc process crashes on Junos platforms when VLANs are deleted and configured PR1831770

General Routing

- The TSC_DEADLINE disabled error logs are observed on Junos vmhost platforms after upgrade PR1608045
- JDI_REG::QFX5200:: After ISSU upgrade, device is hanged and not able to perform any operations until USB recovery done on device PR1703229
- Temporary traffic flooding when root port flaps in all flavours of STP PR1775171
- EX4100 - JUNOS High CPU due to L2ALD PR1780149
- The port class is not captured in cint trace output for individual ports PR1786399
- Master FPC taking 20 sec time to shut backup FPC's network port after backup FPC reboot in a VC set-up PR1788328
- On EX2300/EX3400 series SFP-SX/LX interface is not come up due to auto-negotiation failure PR1789617
- Interfaces down with LOCAL-FAULT alarm after power cycle PR1793137
- [Ex3400] LX/FX SFP Swap leads to traffic drop PR1794986
- ARP won't be forwarded in VLAN associated VNI in VxLAN Fabric PR1801237

- The default port behaviour is not working as expected after deleting VOIP (Voice over IP) configuration on an access interface. PR1802455
- The `set chassis config-button no-clear support` not added on EX4100. PR1802614
- Log messages with LCMD_TMP_SNS_VAL | LCMD_FAN_SET_SPD | LCMD_PEM_FAN_INFO will be observed when syslog is set to "any info" PR1803115
- The dcpfe process will crash in an EVPN-VxLAN scenario due to stale entries in PFE PR1804628
- Establishing virtual-chassis connection between EX4300-MP platforms, the traffic sent via the VCP port is lost minimally PR1805100
- Interfaces remain down on EX4400-48F platform after replacing a 100MB SFP with 1GB SFP PR1805370
- When VC-mode is set to HGOE and converting port type from vc-port to network port, traffic loss is observed PR1806262
- [Optics] EX4100-48MP : Hot swapping 1G SFPT optics ports are not coming up . PR1810482
- Multiple services and protocols does not work on the backup member with 100G port used as VC interconnect port on QFX5110-48S PR1811701
- Persistent MAC getting stuck in the SRP state results in traffic loss in the EVPN-VxLAN scenario PR1812482
- The output of "show chassis routing-engine" does not show the standard documented outputs after a reboot event or a GRES event PR1812514
- EX4400: MIST: Wrong PSU state is updating in the mist PR1814463
- When PDs(power devices) are connected to all the PoE (power over ethernet) ports with LLDP enabled, the last port is not powered up PR1814715
- DHCP snooping issue Observed on Access Ports with IRB and VXLAN Configuration PR1816445
- Switch port status is changed to unauthorized, when a supplicant client attempts to authenticate using 802.1X standard with EAP-TLS certificate PR1819462
- L2TP Processing Issue on EX and QFX Platforms with Tagged CDP VTP and UDLD Frames PR1821012
- The RADIUS attribute NAS-Port-Type is missing from Access-Request packets PR1822101
- Intermittent alarms related to fan overspeed value can be observed on EX4100 platform PR1822363
- MAC address learning fails when Flexible Ethernet Services Encapsulation is enabled on Junos QFX5K and EX4K platforms after a reboot PR1822608

- EX / QFX : dfw ERROR is seen whenever collecting RSI PR1823280
- EX4400-48MXP/48XP CPU hog by Thread CMQFX and Task ACQUIRE_FP_LOCK during PIC offline and online PR1823394
- EX440 series: While performing a 4x25g channelization configuration on the 1x100GE PIC, certain error logs are printed multiple times PR1823743
- In virtual-chassis after routing-engine switchover traffic of type 5 routes of EVPN-VXLAN are not getting forwarded PR1823764
- Restricted Proxy ARP feature does not work as expected PR1824023
- Rebooting one linecard or FPC will cause the virtual-chassis on the EX4K and QFX5K devices to forward traffic in backup RTG interface PR1824750
- EX4400 series: Offline and then an online of PIC 2 installed with a 1x100GE Uplink module configured for Virtual-chassis link causes the link to remain down PR1826147
- System call process stuck in SMbus causing LACP timeouts and affecting all control traffic PR1826615
- After "deactivating protocol dot1x" and activating it again, the dot1x authentication will not work for ports in single/single-secure supplicant mode PR1826621
- Even though installed the license to both Master and Backup, Alarm LED might be lit with yellow on Backup. PR1827641
- EX4400-48MP ping rapid count with high values stops when phone-home is configured PR1828735
- The dot1x client does not get authenticated and gets stuck in the connecting state when a new dot1x profile is assigned along with a newly created VLAN PR1830067
- Commit error on using more than 31 characters authentication-key-chain-name PR1830395
- On an EX4400 device with 4x25G Uplink module configured in 1GE or 25G speed, peer side of an interface with 10GBASE-T transceiver may remain up even when the IFD(xe-x/2/y) is not created PR1831409
- Traffic is impacted due to PFE crash from ukern file logging PR1831813
- On Junos EX4100 and EX4400 platforms, switch core dump when user commits a command to ignore a "power entry module" alarm PR1833698
- MGE interfaces with auto-negotiation enabled and speed negotiated to 5G does not work PR1836616
- Delay in GBP installation in an EVPN-VXLAN scenario PR1839916

- PFE process crash is observed when web-management is not configured in a CWA setup PR1840988
- Traffic blockage observed with SFP-100BASE-BX10 optics in EX4400-48F PR1843585
- Media Access Control Security (MACsec) does not work properly after a transceiver is removed and re-inserted PR1844354
- Interface not added back to AE bundle with multiple changes in single commit PR1845370
- The error message will be seen on EX4100 platforms when deactivating/activating IRB interfaces PR1846286
- Reachability issues are seen on interfaces that are aggregated without address-family PR1847159
- EX4400: Storm-control is created for the GE interfaces for 4x10G uplink modules. PR1848338
- VoIP Phones are unable to receive an IP address with or without dot1x configuration PR1852215
- Devices fail to obtain an IP address when DHCP Security Option 82 is enabled PR1854253
- In Junos EX and QFX platforms, when ERPS protocol is enabled on a ISL trunk, the commit command fails PR1855088

J-Web

- Reload or refresh the Jweb page showing the "Empty reply from server" error PR1832731

Layer 2 Ethernet Services

- Switch provisioned via ZTP going unreachable due to DHCP misbehaviour on upgrading to 21.4R3-S6 PR1808289
- JUNOS_REG:EX4650-48Y:ZTPv6:Failed to reconnect to device as unable to load configuration to device via shelscript from ztp server PR1822178
- DHCP relay option "allow-server-change" does not work as expected in trusted server group when roaming between access points PR1833148
- Unable to assign an IP address on management interface with DHCP configuration even if DHCP is bound after a power cycle PR1854827

Platform and Infrastructure

- Multiple Products: RADIUS protocol susceptible to forgery attacks (Blast-RADIUS) (CVE-2024-3596) PR1802329
- Console login fails when authentication-order is configured under 'system services' hierarchy on all Junos platforms PR1826666
- Multiple Products: RADIUS protocol susceptible to forgery attacks (Blast-RADIUS) (CVE-2024-3596) PR1826678

Routing Protocols

- Junos OS: Multiple vulnerabilities resolved in OpenSSL (CVE-2024-4741, CVE-2024-2511) PR1815253

Subscriber Access Management

- authd process crashes when radius-server-name is configured PR1818321

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

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

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

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

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

Table 2: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for JRR Series

IN THIS SECTION

What's New

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

What's Changed

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

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

IN THIS SECTION

Learn about the issues fixed 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.

General Routing

- CPU utilization of the rpd process stays high on all Junos and Junos OS Evolved platforms PR1808463

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

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

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

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

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

Table 3: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for MX Series

IN THIS SECTION

What's New

IN THIS SECTION

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

To view features supported on the MX Series platforms, view the Feature Explorer using the following links. To see which features are supported in Junos OS Release 24.2R2, click the Group by Release link. You can collapse and expand the list as needed.

- MX240
- MX304

- MX480
- MX960
- MX2010
- MX2020
- MX10004
- MX10008
- MX10016

Additional Features

We have extended support for the following features to these platforms.

- **EVPN-VXLAN Pure Type 5 Stitching with IPv4 Underlay (MX240, MX304, MX480, MX960, MX10004, MX10008, MX10016, MX2010, MX2020)**

  [See Understanding EVPN Pure Type 5 Routes.]

What's Changed

IN THIS SECTION

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

EVPN

- **OISM SBD bit in EVPN Type 3 route multicast flags extended community**—In EVPN Type 3 Inclusive Multicast Ethernet Tag (IMET) route advertisements for interfaces associated with the supplemental bridge domain (SBD) in an EVPN optimized intersubnet multicast (OISM) network, we now set the SBD bit in the multicast flags extended community. We set this bit for interoperability with other vendors, and to comply with the IETF draft standard for OISM, draft-ietf-bess-evpn-irb-mcast. You can see this setting in the output from the `show route table bgp.evpn.0 ? extensive` command.

  [See CLI Commands to Verify the OISM Configuration.]

- **Group-based Policy (GBP) tag displayed with `show bridge mac-table` command**—On platforms that support VXLAN-GBP, the `show bridge mac-table` command now displays a GBP TAG output column that lists the GBP tag associated with the MAC address for a bridge domain or VLAN in a routing instance. Even if the device doesn?t support or isn?t using GBP itself, the output includes this information for GBP tags in packets received from remote EVPN-VXLAN peers.

  [See Example: Micro and Macro Segmentation using Group Based Policy in a VXLAN.]

- **EVPN system log messages for CCC interface up and down events**—Devices will now log EVPN and EVPN-VPWS interface up and down event messages for interfaces configured with circuit cross-connect (CCC) encapsulation types. You can look for error messages with message types EVPN_INTF_CCC_DOWN and EVPN_INTF_CCC_UP in the device system log file **/var/log/syslog**.

General Routing

- Starting from Junos 21.4R1 platforms with the following Routing Engines which have Intel CPUs with microcode version 0x35 observe the error warning, "000: **Firmware Bug**: TSC_DEADLINE disabled due to Errata; please update microcode to version: 0x3a (or later)" on the console. RE-S-X6-64G RE-S-X6-128G REMX2K-X8-64G RE-PTX-X8-64G RE-MX2008-X8-64G RE-MX2008-X8-128GPR1783225

- Change to the commit process—In prior Junos OS and Junos OS Evolved releases, if you use the commit prepare command and modify the configuration before activating the configuration using the commit activate command, the prepared commit cache becomes invalid due to the interim configuration change. As a result, you cannot perform a regular commit operation using the commit command. The CLI shows an error message: 'error: Commit activation is pending, either activate or clear commit prepare'. If you now try running the commit activate command, the CLI shows an error message: 'error: Prepared commit cache invalid, failed to activate'. You then must clear the prepared configuration using the clear system commit prepared command before performing a regular commit operation. From this Junos and Junos OS Evolved release, when you modify a device configuration

after 'commit prepare' and then issue a 'commit', the OS detects that the prepared cache is invalid and automatically clears the prepared cache before proceeding with regular 'commit' operation.

[See Commit Preparation and Activation Overview]. PR1806197

- When you run the `run show lldp local-information interface interface-name | display xml` command, the output is displayed under the lldp-local-info root tag and in the lldp-local-interface-info container tag. When you run the `run show lldp local-information interface | display xml` command, the lldp-tlv-filter and lldp-tlv-select information are displayed under the lldp-local-interface-info container tag in the output.

- Change in use of RSA signatures with SHA-1 hash algorithm?Starting in Junos OS Release 24.2R1, there is a behavioural change by OpenSSH 8.8/8.8p1. OpenSSH 8.8/8.8p1 disables the use of RSA signatures with SHA-1 hash algorithm by default. You can use RSA signatures with SHA-256 or SHA-512 hash algorithm.

- For MPC5E line card with flexible-queuing-mode enabled, queue resources are shared between scheduler block 0 and 1. Resource monitor CLI output displays an equal distribution of the total available and used queues between scheduler blocks. This correctly represents the queue availability to the routing engine.

- **Enhancement to fix output with Junos PyEz for duplicate keys in PKI (MX Series, SRX Series, EX Series)**—In earlier releases, though the CLI output displayed all the duplicate keys for the corresponding hash algorithms in PKI using `show security pki local-certificate detail | display json` command, for the same requested data, Junos PyEz displayed the last key only. Starting this release, the CLI output and the PyEz displays all the duplicate keys with the enhanced tags.

  PR1811508

- In a firewall filter configured with a port-mirror-instance or port-mirror action, if l2-mirror action is also configured, then port-mirroring instance family should be any. In the absence of the l2-mirror action, port-mirroring instance family should be the firewall filter family.PR1818423

- Support added for interface-group match condition for MPLS firewall filter family. PR1818968

- Licensing (MX Series)-The PWHT for layer 3 VPNs or BNG feature moved from premium tier to advanced tier.PR1843429

- The CVBC does not require any documentation. As described in the assessment tab, there is a change to the warning message displayed on the CLI. We don't usually document warning messages displayed on the CLI.PR1856239

Junos OS API and Scripting

- **Changes to the XML output for ping RPCs (MX480)**—We've updated the `junos-rpc-ping` YANG module and the corresponding Junos XML RPCs to ensure that the RPC XML output conforms to the YANG schema. As a result, we changed the XML output for the following ping RPCs:
  - `<ping>`—The XML output emits `<ping-error-message>` and `<ping-warning-message>` tags instead of `<xnm:error>` and `<xnm:warning>` tags.
  - `<request-ping-ce-ip>`—The XML output is enclosed in an `<lsping-results>` root element.
  - `<request-ping-ethernet>`—
    - The `<ethping-results>` root tag includes a `<cfm-loopback-reply-entry>` or `<cfm-loopback-reply-entry-rapid>` tag for each received response. In earlier releases, a single tag enclosed all responses.
    - The XML output includes only application specific error tags and omits `<xnm:error>` tags.
    - The `<cfm-loopback-reply-entry-rapid>` tag is now reflected in the YANG schema.
  - `<request-ping-overlay>`—The `<ping-overlay-results>` element includes a new child tag `<hash-udp-src-port>`.

Routing Protocols

- **Update to IGMP snooping membership command options**— The `instance` option is now visible when issuing the `show igmp snooping membership ?` command. Earlier, the `instance` option was available but not visible when `?` was issued to view all possible completions for the `show igmp snooping membership` command.

  [See show igmp snooping membership.]

- **Extension of traceoptions support for VLANs in IGMP/MLD snooping**— The `traceoptions` option is supported under the `[edit routing-instance protocols igmp-snooping vlan]` and `[edit routing-instance protocols mld-snooping vlan]` hierarchy. `traceoptions` can be enabled for both specific and all vlans.

  [See vlan (IGMP Snooping)].PR1845242

Subscriber Access Management

- You can configure VLAN termination cause codes to specify RADIUS attribute values for different termination scenarios on Junos OS MX Series platforms supporting the Layer-2 Bitstream Access

(L2BSA) feature. You can diagnose and manage network issues effectively by understanding the specific reasons for VLAN termination. Ensure that the correct termination cause codes are sent by validating configuration and testing scenarios to correctly interpret network events. When a subscriber logs out, the system occasionally sends an incorrect termination cause value to RADIUS. The subscriber VLAN "Account-Terminate-Cause" in "Acct-Stop" message for different L2BSA subscriber logout error scenarios is modified to display correct reasons for termination.

[See "VLAN Termination Causes and Code Values" and "show network-access aaa terminate-code"].PR1854701

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.

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the `Hostname` field first instead of last. The `show version` command output includes the `Family` field. The `Family` field identifies the device family under which the device is categorized, for example, `junos`, `junos-es`, `junos-ex`, or `junos-qfx`.

  [See show system information and show version.]

- **Access privileges for request support information command (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance`, `view`, and `view-configuration` can execute request support information command.

  PR1835092

VPNs

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

  [See min-rate.]

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

  [See min-rate.]

Known Limitations

IN THIS SECTION

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

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

General Routing

- The time delay on GNF reconnect is due to socket drop on alarmd and chassis went for a reconnect, during this reconnect process the ready messages from GNFs are ignored until the chassis reconnect timer is expired. The socket drop on alarmd and reconnect is expected while performing GRES. PR1771319

- The error message received IFD attach for interface name with PIC in Offline or Offline wait state.Ignore it , IFFPC: ifd detach returned error 7 is usually observed when a PIC reconfiguration is triggered while the IFDs are still getting installed at the linecard. PIC reconfiguration is mainly due to a PIC mode change. Before triggering a pic mode change, in addition to checking the state of the pic mode that is, if the PIC is online, also verify that the IFDs are attached correctly either by allowing adequate delay between PIC bounce (approximately 3 to 5 minutes) or observing logs.PR1774974

- The error message is observed when a PIC reconfiguration is triggered while the IFDs are still getting installed at the linecard. PIC reconfiguration is mainly due to a pic mode change. Before triggering a pic mode change, in addition to checking the state of the pic mode i.e if the PIC is online, also verify that the IFDs are attached correctly either by allowing adequate delay between PIC bounce (~3-5mins) or observing logs.PR1780251

- L2cs upgrade failure occurs when you run the jfirmware upgrade. PR1783364

- If SGRP over subscription is configured for a BNG-UP port which hardware doesn't support over subscription it still accepts the port into the SGRP. The result is subscribers are not handled properly. PR1791676

- 1PPS performance drop is seen during clksyncd process restart with 1588 default profile. Its a baseline Mx Aloha line card behaviour. PR1796244

- `show system license` output does not display hardware based licensing details. `show system license bandwidth flex-only` output displays linecard specific bandwidth details. It makes the calculation very complicated to add advance/premium details to this output. Tier can be chassis, linecard or port based. Bandwidth details is for all ports of the linecard irrespective of the tier of each port.PR1797309

- When we first create a route record in the client DB, the Berkeley DB (BDB) module opens a file and creates a record. Now, if there are two REs, the BDB module will sync this DB file to the backup RE. Till now, the file management is being exclusively handled by the BDB module. Now, if the client deletes all the routes and goes away and now if PRPD tries to do the file management instead of Berkeley DB and deletes the file, it can do this only on the master RE. Now, if the RE switchover happens, the DB file will still exist in the backup RE. Juniper's BDB module is responsible for managing the files and it doesn't provide a remove function which will keep the files in sync across master and backup RE.PR1801509

- MPC11 In-Service-Software-Upgrade command fails from Junos OS release 24.1R1 to 24.2R1 and causes MPC11 linux crash. The issue only applies to ULC image.PR1803205

- 40g interface doesnt support EM policy feature but it will still display in the cli output of `show chassis temp-threshold` as it gets created as "et" interface. PR1807219

- MX Bandwidth alarms are refreshed at the configured log interval (default 06:00AM). Any usage changes within this interval which maintains license non-compliance will not raise new alarms just for the changed in license-needed value. Real time license-needed value is updated in the output of "show system license"PR1853132

Layer 2 Ethernet Services

- Issue was seen when test was done back to back GRES within 5mins time. this is expected behavior from the system as per current architecture. Suggestion is to wait for sometime before maybe 10 minutes or so for subsequent GRES. PR1801234

Platform and Infrastructure

- When global level changes are made like changing Mac-age, with large scale and high CPU a watchdog core is generated without any functional impact. The config change is pushed from l2alm to pfe, which loops through all the RTTs and associated bd and ifbd. If the process is not yielded within 240sec, the pfeman watchdog is called in and writes a core. PR1775966

Routing Protocols

- On Junos and Junos Evolved platforms, protocol isis is supported a rare display issue is seen ISO address is not being picked up properly and Sysid is not showing the proper valuePR1726823

Services Applications

- In Junos OS Release 17.4 and later, 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

Open Issues

IN THIS SECTION

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

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

EVPN

- On all MX Series platforms the deactivation a routing-instance configured with 'vrf-target auto' while also configured with protocol EVPN leads to the rpd crash in all the Routing Engine present in the chassis. PR1821582

Forwarding and Sampling

- In case of filter-base forwarding (FBF) which filter has 'then routing-instance' action term, firewall filter will not work properly after deactivate/activate the routing-instance being done. Even any config is not changed before and after deactivate/activate the routing-instance, packets will not be forwarded to packets' destination device.PR1810237
- Whenever the CBS was configured above its limit (earlier 33m), the low-level parameters used to get configured such that the packets would not have any credits available, resulting in them getting marked as RED.PR1837840

General Routing

- You might see a misleading syslog message "L2CKT/L2VPN acquiring mastership for primary" although no VPN/L2CKT is configured on the router. PR1105459
- For the MPC10E card line, the IS-IS and micro-BFD sessions do not come up during baseline. PR1474146
- In Sync-E configuration, Config 1: ESMC transmit is configured Config 2: if deactivated chassis synchronization source configured OR no chassis synchronization source is configuring is active then commit error is given as "'esmc-transmit' requires 'chassis synchronization source' configuration". PR1549051
- 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
- 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
- Percentage physical-interface policer is not working on aggregated Ethernet, after switching between baseline configuration to policer config uration.PR1621998
- On all Junos OS platforms, agentd process crash will be seen in telemetry streaming longevity test.PR1647568
- 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
- %PFE-x: fpcx user.err ppman: [Error] PPM:PROCESSOR_L2TP_SF: PpmProcProtoL2tpSf::processPkt: No tunnel entry found for received L2TP tunnel control packet. LocalAddr: x.x.x.x LocalTunnelId: 0 Timestamp xx:xx:xx device fpcX user.err ppman: [Error] PPM:PROCESSOR_L2TP_SF: PpmProcProtoL2tpSf::processPkt: Received packet Ipv4 header parsing failed. PacketSize:xxPR1689921
- On Junos OS 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 LAG is configured with mixed speed interfaces switching to a secondary interface of different port speed, results in a few packet drops for a very short duration. PTP remains lock and there is no further functional impact. PR1707944

- Support of "no-confirm" option in ISSU so as to avoid the interactive prompts. This is to suppres the user prompts and proceed for restart upgrade for hitless kernel restart upgrade. If there is any error which can impact traffic then abort the upgrade.PR1713589
- Once the device is loaded with the new image, PIC tries to boot up. mspmand is one of the processes inside PIC, crashes sometimes.PR1714416
- fec-codeword-rate data with render type decimal64 is rendered as string in grpc python decoder.PR1717520
- 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
- Telemetry Stats are not visible for MPLS LSP(RSVP-based) when the core interface is MPC11/ MPC10.PR1731587
- PTP state went to Freerun and acquiring before phase-aligning again when the SyncE ESMC is disabled or downgraded from GM or the upstream node one hop above the parent node. PR1738532
- On MXVC , Due to some timing issue when RPD is restarted, It will not be spawned again. This issue is rarely reproducible.PR1740083
- Error message might occur once in a while with full scale during negative scenarios like 'clear bgp neighbor all' with all the services like EVPN, vrf etc being present.PR1744815
- RBU DIAGS REGRESSIONS: MX480 CommonDiag::JDE3(volt_services_show_clients) failing on MPC7e. PR1747033
- 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
- RBU DIAGS REGRESSIONS: MX2010 Diagnostics::Jde3Diag(phy_reg_access) test is failing. PR1747297
- On all MX Series platforms, faulty hardware issue on MIC due to clock sync error generated brings down the interfaces without any major alarm or log notification.PR1749943
- On MPC10E line cards based MX Series platforms with aggregated Ethernet interface configured with Link Aggregation Control Protocol (LACP), subscriber management and auto-configure statement enabled, ping to neighbour fails post swapping member-interfaces between two AE (one

with VLAN configuration and the other without VLAN configuration). Traffic forwarding on respective interfaces will be impacted as interface is moved from AE having VLAN to AE not having VLAN.PR1751260

- On all Junos OS Evolved platforms and device with MX10K-LC2301/ MX10K-LC9600, MX304,LC480,LC2101,LC1201 the voltage threshold cross is reported by MX20796 sensor. PR1752654
- On Junos MX Series platforms with Trusted Platform Module (TPM), reset of master password got stuck post device reboot. PR1760822
- On MX Series platform with a combination of MPC1-9, LC480, LC2101, and MPC10E, MPC11E, LC9600 line cards, when preserve-nexthop-hierarchy knob enabled and maximum-ecmp configured with more than 32 next-hops in the MPLS FRR (Multiprotocol Label Switching fast-Reroute) and BGP (Border Gateway Protocol) Multipath scenario, packet loss when primary path is added back in ECMP nexthop (say after primary interface or session is marked UP) will be higher compared to that on MX platform with MPC1-9, LC480, LC2101 line cards only, OR with MPC10E, MPC11E, LC9600 line cards only. This packet loss is proportional to the value in maximum-ecmp configuration.PR1765856
- On Junos OS platforms, when executed just after line-cards are up after system-reboot, the CLI output for active-errors (show system errors active, show system errors active detail) displays empty output for some initial duration that can run for minutes. Issue is seen when number of errors present in line-card is very high (10K+). Since all these errors need registration with CLI serving daemon running on Routing Engine, before it can display error-info, CLI output for this command is delayed. However, as a workaround alternative CLI (`show chassis errors active detail`) can be used, which displays similar output. PR1775073
- Issue identified when upgrading vmhost, but applies to all Junos OS platforms that support vmhost. When there are tar errors during the upgrade, and the reboot option is used in the upgrade command, the machine will still reboot the Routing Engine despite that the upgrade was not completed correctly. This will break the routing engine. It is necessary to stop the reboot, if error or tar problems occurred during the upgrade.PR1770585
- On Junos platforms, when executed just after line-cards are up after system-reboot, the CLI output for active-errors (show system errors active, show system errors active detail) displays empty output for some initial duration that can run for minutes. Issue is seen when number of errors present in line-card is very high (10K+). Since all these errors need registration with CLI serving daemon running on RE, before it can display error-info, CLI o/p for this command is delayed. However, as a workaround alternative CLI (show chassis errors active detail) can be used, which displays similar output.PR1775073
- Junos (JET) telemetry that is pre-gNMI telemetry that uses sensors that are of a double data type are converted to a float data type when streamed to a collector.PR1777319

- Commit error is needed when streaming server and export-profile is not configured properly. With the incomplete configuration that is missing below might cause the interfaces to go down upon reboot of the unit or FPC. `set services analytics streaming-server profile name remote-address ip set services analytics streaming-server profile name remote-port port set services analytics export-profile profile-name reporting-rate rate`. This needs to be greater than 1.PR1779722

- Even after `request vmhost power-off` LEDs keep lighting on. The LEDs state should be off because routing-engine doesn't have power in case of `request vmhost power-off`.PR1781815

- The `show` command cause performance degradation or hog CPU. PR1784219

- V6 Endpoint SRTE: 4PE (IPv4 over IPv6) routes in inet.0 table are not getting resolved in inet6color table because 4PE is not supported with inet(6)color model. 4PE can be supported with transport class. PR1786029

- On MX100008 and MX100004, if 25G and 50G optics are JIJO within 1 second manually, then sometimes the interface does not come up. As a workaround, do not JOJI within a 1 second time period. It is recommended that the duration between JIJO is minimum 3 seconds.PR1786404

- Additional logging has been added to the primry Routing Engine. This is to help narrow down the issue which chassisd process restarted unexpectedly at snmp_init_oids( ) function on the primary Routing Engine while booting up.PR1787608

- When interfaces with different speed are configured as members of AE, some of the members are not added to aggregated Ethernet. And if GRES is enabled, vmcore might be generated on backup Routing Engine. PR1799451

- Under scaled configurations with interfaces, FW filters, routing protocols etc certain script based config/unconfig automated operations, in the presence of continuous traffic, can encounter one or more PPE traps that momentarily cause traffic drops. These momentary traffic drops happen at the tail end of the time the business configuration is removed and a baseline configuration is loaded in a single commit. These do not cause any service or functionality impact. PR1800967

- Due to a the disk failure reboot support was not added for dual disk scenario, hence system was not booting in case of disk failure on sdb (the other disk) on QFX platform.PR1800862

- On all MX platforms(except MX80) with multi line card chassis, when PTP slave or stateful streams are configured across multiple linecards with clock from same PTP time provider and the announce msg parameters changes from the upstream device, the best master clock (BMC) slot switchover is observed and is restored back within few seconds. Although the slot time interval is very less, it can still lead to major impact as the active PTP slot and clock path is switched over and results in re-routing of the clocks.PR1803105

- MPC11 ISSU command fails from Junos OS Release 24.1R1 to 24.2R1 and causes MPC11 linux crash. The issue only applies to ULC image.PR1803205

- This issue is caused because of the fact that peers-synchronize is configured, and master-password is configured to encrypt the config being sync'ed. However, as there is no master-password configured on the peer device, the encrypted configuration cannot be decrypted (this is expected). This has not been supported from day-1, however a workaround can be done in order to get this to work. The workaround is to manually configure the same master password on the peer device manually. At a high level the problem is as follows: Consider there are two devices A and B in a peer-sync config 1. config on dev A contains secrets which need to be encrypted with the master password and synced with the device B 2. The master-password (juniper123+masterpassword) is configured on device A and the configuration is encrypted and written to /tmp/sync-peers.conf 3. The /tmp/sync-peers.conf is then synced to device B but device B does not have the same master-password configured which results in the config failing to decrypt. The master-password itself is not a part of the config-database. Additionally, it cannot be transmitted over an unencrypted HA Link, as this would lead to the master-password getting leaked. This is by design, and would be a security concern if it were to be transmitted across an unencrypted channel. Therefore, this work as designed. In order to work around this issue follow these steps: 1. configure the master-password on device B and commit the config 2. configure the same master-password on device A and commit the config and it should get sync'ed correctly.PR1805835

- PLL Access Failure alarms is observed on a MPC11E line card of REV 53 after loading 24.2I-20240429.0.0958 on a MX2010 boxPR1808044

- Feature names will be used across license alarms and logs generated. This has a 1:1 mapping to the feature names used in output of 'show system license' command.PR1808084

- `set chassis no-reset-on-timeout` is a debug command for SPC3 to prevent it from rebooting in case of issue. It is not to be set during normal operations since SPC3 may need reboots to come online.PR1809929

- Traffic loss will be seen on 1G-SFP-T if speed is configured to 100m. 1G SFP-T has the AN feature enabled but the PHY we have b/w SFP-T and switch ie., PHY82756 doesn't support AN and this mismatch is causing the traffic loss. This needs feature enhancement PR1817992

- On MX Series platforms with MS-MPC and Carrier-Grade Network Address Translation (CGNAT) configured, a large number of "out-of-address" errors and stale NAT mappings for SIP (Session Initiation Protocol) traffic can occur. This can lead to a lack of available resources and cause new connections to be dropped.PR1826847

- As per OpenSSH 9.0/9.0p1 release notes: "This release switches scp(1) from using the legacy scp/rcp protocol to using the SFTP protocol by default." In this case, since we are running OpenSSH 9.0 and above- OpenSSH_9.7p1 , this uses the "SFTP" protocol by default when scp command is invoked from shell. However, vSRX3.0 supports the "SCP" protocol by default when scp command is invoked. So to use the legacy "SCP" protocol from shell, please use the -O command line option For example: scp -O other options or arguments Note: Incoming SCP connections from outside hosts that are running OpenSSH version greater than or equal to 9.0/9.0p1 could fail since sftp-server is disabled by default in Junos OS . Hence, users should either use the -O option on remote host while initiating

scp file transfer OR enable sftp-server in the Juniper configuration. To enable sftp-server in Juniper configuration, use the following hierarchy: "set system services ssh sftp-server". PR1827152

- When the other RE is rebooted/removed the following alarm is observed "Host 0 bme1 : Ethernet Link to other RE Down". Alarm is observed as long as the other RE doesn't come back online. The alarm goes off once the other RE boots up / inserted. This is a part of the periodic which checks for the other RE connectivity. There is no functional impact with the alarm since it is cleared once the other RE comes back online.PR1840810
- There will be no impact on traffic, problem on displaying extra lanes in SNMP query.PR1844751
- We do not recommend to use ":" in instance name configuration as it is considered as reserved for internal use. PR1849070
- Customer is using the Dot1x RADIUS authentication and accounting and noticed that when the Stop Accounting(due to disconnect) is sent to the RADIUS server the Acct-Input-Gigawords and the Acct-Output-Gigawords is having huge value as below which is not expected. AVP: t=Acct-Input-Octets(42) l=6 val=0 AVP: t=Acct-Output-Octets(43) l=6 val=0 AVP: t=Acct-Session-Time(46) l=6 val=12 AVP: t=Acct-Input-Packets(47) l=6 val=520538 AVP: t=Acct-Output-Packets(48) l=6 val=2106672 AVP: t=Acct-Terminate-Cause(49) l=6 val=Admin-Reboot(7) AVP: t=Acct-Input-Gigawords(52) l=6 val=60519852. (AVP: t=Acct-Output-Gigawords(53) l=6 val=185322927)PR1851299
- On all Junos and Junos Evolved platforms this is an enhancement for Nexthop APIs to support LDP stitching cases over BGP routes pointing to list of indirects next-hops.PR1851629

High Availability (HA) and Resiliency

- Graceful Routing Engine Switchover (GRES) not supporting the configuration of a private route, such as fxp0 , when imported into a non-default instance or logical system. Refer to KB26616 resolution rib policy is required to apply as a work-around.PR1754351

Interfaces and Chassis

- JUNOS MX | iflset stats not getting cleared after issuing clear interfaces stats all and clear interfaces interface-set statistics all CLI commandPR1741282

Junos XML API and Scripting

- On all Junos OS platforms where snapshot is supported, when a device is rebooted from recovery mode it fails to commit configuration due to problems with slax import and device might go into amnesiac mode due commit fail.PR1717425

Layer 2 Ethernet Services

- On MX Series platforms in the Dynamic Host Configuration Protocol (DHCP4) and DHCPv6 subscribers in ALQ (Active Leasequery) EVPN-VPWS (Ethernet VPN - Virtual Private Wire Service) without topology-discover scenario, due to incorrect GIADDR (Gateway IP address) DHCP-OFFER gets dropped leading to subscribers not completing the DORA (Discover, Offer, Request, Acknowledge) process. The issue seen for static PS (Pseudowire Service) VLAN interfaces where DHCP subscribers are landing.PR1763331

- In order to allow protocol daemons (such as rpd, dot1xd et. al.) to come up fast when master password w/ TPM is configured, the daemons must be allowed to cache the master-password when they read their configuration. In order to cache the master-password, the daemons must individually reach out to the TPM to decrypt the master password and cache it in their memory. This scenario leads the TPM to be flooded with decryption requests, and therefore causes the TPM to be busy and start rejecting decryption requests. To prevent the daemons from core dumping in this scenario, and to allow successful decryption of secrets, we retry the decryption request to the TPM. However, to allow the TPM queue to drain, we introduce a sched_yield() call before retrying to sleep for 1 quantum of time. Without this, we will fail on all our retries. Additionally, a decryption request can also take a large amount of time (> 5 secs). This results in SCHED_SLIP messages being seen in the logs, as the requesting process is idle while the decryption request is being processed by the TPM. This can exceed the SCHED_SLIP timeout, and result in libjtask logging the SCHED_SLIP messages into the configured system log file. These SCHED_SLIPs should not cause any route instability, are benign, and can be ignored as these are seen only during configuration consumption by the various daemons.PR1768316

- DHCP-Relay short cycle protection can get stuck in Grace periodPR1835753

Network Management and Monitoring

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

- Issue: Multiple traps are generated for single event, when more target-addresses are configed in case of INFORM async notifications Cause: INFORM type of async notification handling requires SNMP

agent running on router to send a Inform-Request to the NMS and when NMS sends back a get-response PDU, this need to be handled. In this issue state, when more than one target-address(NMS IP) is configured for a SNMP v3 INFORM set of configuration, when Get-Response comes out of order in which the Inform-Request is sent, the PDU is not handled correctly causing snmp agent to retry the Inform-request. This was shows as multiple traps at the NMS side. Work-around: For this issue would be to use 'trap' instead of 'inform' in the "set snmp v3 notify NOTIFY_NAME type inform" CLI config.PR1773863

Platform and Infrastructure

- Heap memory leak on access MPCs used for subscriber termination may be observed in a subscriber-management environment.PR1732690
- PCT-VIRTUAL: Firewall filter counters are not incremented as expected when filter is applied to IRB interface in the ingress/egress direction via forwarding tablePR1766471
- "Possible out-of-order deletion of AftNode" error messages will be seen after ifconfig down/up. Issue is seen due to out-of-order IPCs received for IRB MACs. This causes the MAC entry not to be deleted from the s/w MAC table which prevents the deletion of associated NH token. 30 minutes post the ifconfig down/up, the error messages will be seen.PR1815922

Routing Protocols

- LDP OSPF are in synchronization state because the IGP interface is down with ldp-synchronization enabled for OSPF. user@host> show ospf interface ae100.0 extensive Interface State Area DR ID BDR ID Nbrs ae100.0 PtToPt 0.0.0.0 0.0.0.0 0.0.0.0 1 Type: P2P, Address: 10.0.60.93, Mask: 255.255.255.252, MTU: 9100, Cost: 1050 Adj count: 1 Hello: 10, Dead: 40, ReXmit: 2, Not Stub Auth type: MD5, Active key ID: 1, Start time: 1970 Jan 1 00:00:00 UTC Protection type: None Topology default (ID 0) -> Cost: 1050 LDP sync state: in sync, for: 00:04:03, reason: IGP interface down config holdtime: infinity. As per the current analysis, the IGP interface goes down because although LDP notified OSPF that LDP synchronization was achieved, OSPF is not able to take note of the LDP synchronization notification, because the OSPF neighbor is not up yet. PR1256434
- On MX Series platforms, unexpected log message will appear if the CLI command 'show version detail' or 'request support information' is executed: test@test> show version detail *** messages *** Oct 12 12:11:48.406 re0 mcsnoopd: INFO: krt mode is 1 Oct 12 12:11:48.406 re0 mcsnoopd: JUNOS SYNC private vectors set. PR1315429
- On all Junos OS platforms and Junos Evolved with scaled BFD sessions, FPC reload/restart results in few BFD session flap.PR1698373

- On all Junos and Junos OS Evolved platforms, multiple simultaneous Command Line Interface (CLI) sessions will lead to high Management Daemon (mgd) CPU utilization, impacting the device's reachability over the loopback interface from IS-IS nodes.PR1749850
- With BGP sharding and NSR configured , deactivate/activate routing-instances and interfaces was done back to back multiple time on active RE, leads to the rpd core on backup RE at rt_flash_queue_insertPR1781293
- Configuration of a global AS number is necessary when route target filter is enabled. Currently JUNOS cli does not enforce configuring a global AS number and it has been the behavior for a long time. Many unexpected issues may be seen without a global AS number. It's been a recommended practice to configure a global AS number in the field.PR1783375
- Loading ROAs from a source-file was a feature introduced as a convenience feature and as such this only affects that feature. This feature is not in widespread use and was created to have a fallback ROA when all sessions go down. This problem scenario requires multiple reloads with the file.cbor being modified back and forth to add and then delete and re-add the database configured in the import policy.PR1853025

User Interface and Configuration

- To recover from this and to avoid problem due to problem delta synchronize, "set system commit no-delta-synchronize" can be configured as work-around (no-delta-synchronize is hidden knob but safe to use). It will enforce entire ?juniper.conf? to synchronize rather than delta changes and will help in this case.PR1801136
- Upgrade from Junos OS Release 20.3x to 24.2R1 fails if extend-db config stanza is present This issue is happening due to extend-db knob configured in the config. Delete the extend-db knob, reboot the box and then perform the upgrade. Issue is not seen. PR1806109 and PR1807931
- After switchover in MX2010 platform , test config is removed with load update and then rollbacked. during rollback commit , config commit failed with below error: error: commit-check-daemon : Invalid XML from dfwd error: configuration check-out failedPR1829614

VPNs

- As part of non-ZPL ISSU, traffic loss of max 2secs is expected due to the dark window. PR1797403

Resolved Issues

IN THIS SECTION

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

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

Class of Service (CoS)

- Multiple adjacencies may get dropped over AE interfaces PR1828018
- FC id goes out of sync between the RE and PFE impacting all CoS features using FC id PR1836528

EVPN

- MHPE sets as I_ESI instead of RNVE in EVPN-VXLAN configurations without the DCI interconnect configuration. Receiver sees traffic hop between source-VLAN and SBD PR1799761
- VXLAN/EVPN ip-address for mac-address in forwarding table in hold state PR1802464
- The MAC pinning functionality is not working on QFX platforms PR1806416
- The VXLAN traffic drop could be seen after modifying control-word in an EVPN instance PR1807084
- The rpd process will crash when TTE is enabled with EVPN-VPWS or EVPN-ELAN configured PR1808180
- EVPN over MPLS IPv6/SRv6: PMSI attribute carrying wrong flags with value 0x20 (bit 2). PR1814525
- Continuous kernel log messages are observed once the EVPN-VXLAN fabric is up PR1826772
- GBP tags remain in place even after GBP tag assignment firewall filter is removed or deletion of mac-ip entry on specific Junos EX and QFX platforms with EVPN-VXLAN PR1830126
- [EVPN] The one of routing-instances configuration changing affects whole LACP state under "lacp-oos-on-ndf"(LACP out-of-sync) and EVPN "single-active" conditions. PR1832785
- RPD restart immediately on EVPN Designated Forwarder PE with Graceful-restart results in 100% traffic loss for 12-15 secs PR1846096

Flow-based and Packet-based Processing

- Junos OS: SRX4600, SRX5000 Series: TCP packets with SYN/FIN or SYN/RST are transferred after enabling no-syn-check with Express Path (CVE-2024-39561) PR1776940
- On SRX Series devices, when using IPv6 Multi-path BGP with MX configured with EVPN, transit SFW traffic experiences packet drops during IPv6 Neighbor discovery refresh. PR1817211

- Junos OS: SRX4600 and SRX5000 Series: Sequence of specific PIM packets causes a flowd crash (CVE-2024-47503) PR1820291

Forwarding and Sampling

- Wedge condition is seen on MX platforms with MPC10/MPC11/JNP10K-LC9600 and MX304 platform switch port utilization is above 80% PR1800623
- Empty commit is behaving as commit full after the system was upgraded PR1818988
- A BFD flap and subsequent impact in the traffic is seen when BGP FlowSpec session goes down or withdrawal of all BGP FlowSpec routes making entries on netflow.0 table to zero at once PR1827439

General Routing

- The TSC_DEADLINE disabled error logs are observed on Junos vmhost platforms after upgrade PR1608045
- Multiple J-UKERN core files might be generated during the sanity test PR1641517
- On MX10004/MX10008/MX10016 chassis running Junos LC480 may reboot when "show system firmware" CLI command is executed to get the firmware information PR1696186
- Observing core with rpd with BGP flowspec if secondary-independent-resolution is configured PR1722715
- JDI-RCT:M/Mx: SMPC crash @ hostif_clear_toe_interrupts, toe_interrupt_handler after fpc restart scenario . PR1733053
- On MPC10E after frequent interface flaps, interface does not come up PR1735539
- with BGP sharding , observed memory leak in cookie ifx_dist_msg PR1761238
- Junos OS: Due to a race condition AgentD process causes a memory corruption and FPC reset (CVE-2024-47494) PR1769294
- The max allocated power numbers are lower than the recommended values PR1770642
- Temporary traffic flooding when root port flaps in all flavours of STP PR1775171
- FPC gets stuck at 100% utilization after upgrade from 21.2R1 or below to 21.3R1 or higher release PR1777139

- EX4100 - JUNOS High CPU due to L2ALD PR1780149
- Subscribers wont't be able to login when a new VLAN range is added under dynamic profile PR1782374
- The mspmand process might crash on the MS-MPC during deletion of service-sets configuration PR1783745
- Dvaita GNF with MPC11 card Jvision stats exported has wrong system id. PR1784806
- Redundancy Support for New Consumer Services / BNG Licensing on Junos OS MX Series platforms. PR1787234
- Traffic drop due to mac-validate failure on MX Series platforms. PR1788669
- An enhancement to modify the output and alarm when an interface is down due to XCVR over temperature PR1789622
- Configuring multiple IFL of different families on Junos QFX10K SP style interfaces leads to traffic loss PR1792128
- Interfaces down with LOCAL-FAULT alarm after power cycle PR1793137
- CMErrors are observed on MX platforms running MPC10/MPC11 causing the PFE to be disabled PR1793375
- NSD coredump is seen on MX Virtual-Chassis every time when MXVC reboot if [service-set() flow-log] is configured PR1793765
- Traffic impact during ISSU across FPCs on Junos MX platforms PR1796770
- We may observe repd core (in the "from" release) during ISSU. There are no functional impact due to this repd core PR1797189
- The system goes into a bad state when an SFB ungraceful offline happens due to a fatal Interrupt PR1798780
- VNF OVS Interface failure with high memory PR1799045
- The "show chassis synchronization clock-module | display xml validate" get "INVALID" output PR1799397
- Traffic loss observed when we configure more then 256 terms in Fast-lookup-filter PR1799457
- Traffic impact on SPC3-PIC due to high throughput and bursty traffic PR1799512
- jti/plugin: The certificate of existing junos plugin pkgs (foo_plugin and bar_plugin) are expired and need the new ones PR1800642

- xSTP does not work in ephemeral-db mode on all Junos OS Evolved platforms after the l2cpd restart PR1800645
- On Junos platforms the telemetry subscribe to path": "/components/component[name='Routing Engine0']/state/memory/utilized is not working as expected PR1800754
- PEM1 alert is going to clear immediately, and alarm LED was not lit after the power cable/PEM was removed. PR1800855
- Traffic drop is observed when an SP style port is added to an existing vlan lag interface PR1801217
- The RE switchover will not be triggered in case of clock failure on SCBE3-MX PR1801284
- Crash files are generated every 24 hours due to a pkid process crash PR1801377
- Memory Leak in the rpd Process During Protocol Deactivation/Activation PR1801382
- SFB PCIE switch temp sensors yellow alarm falsely reported at high altitude and high temp operating conditions PR1801778
- Parameters on xSTP interface were not as expected after switchover PR1801786
- The optics temperature sensor name renamed from 'et-x/y/z' to 'xcvr-x/y/z' PR1802195
- Interim logs for deterministic NAT are not generated as per the modified time interval PR1802242
- AFTD crash may be observed when a MAJOR CMERROR that affects only one of the slice of a multi-slice PFE is triggered PR1802243
- SFB ungraceful offline followed by master SPMB reboot results in traffic drops due to fabric Link errors PR1802259
- Filter will be configured with incorrect vlan-IDs and commit error will not be displayed PR1802362
- PTX10008 - Recurring logs -ppcfpc-multi-svcs.elf: FDB :: Ipv4 route operation 2 failed. Rt_index 1801 PR1803542
- MPLSoUDP route issue preventing LSP establishment PR1803578
- Traffic loss is observed along with error messages on Junos MX platforms with MPC1 to MPC9, LC2101, LC480 (including MX10003) during any transport LSP change operation PR1804263
- The rpd process crash can be seen in restoration to baseline configuration in scaled scenario PR1804363
- NSD validation failure results into upgrade failure for Junos MX platforms PR1804616
- The dcpfe process will crash in an EVPN-VxLAN scenario due to stale entries in PFE PR1804628

- The rpd process crashes during rpd restart on Junos and Junos Evolved platforms PR1805427
- Return Error for unsupported options with GNMI RPCs PR1805445
- show snmp mib walk jnxFruTemp is NOT correctly updated for PEM components PR1805483
- Telemetry stats for af interfaces are not getting streamed for UKERN based Linecard PR1805769
- Interfaces fail to coming up on ACX EVO platforms after deleting the routing-instance with DHCPv6 and adding new configuration on same interface PR1806148
- Chassis not recovering clock from GM, but still advertisement of GM provided clock-class to downstream node PR1806526
- MX platforms with with MPC10,MPC11,LC9600 and MX304 we observe IPv6 unilist next-hops are missing PR1806717
- Partial traffic blackhole will be observed during the time of FPC crash due to interfaces not going down PR1806787
- SFB power off/unplug followed by ungraceful SPMB restart leads to SPMB crash PR1807410
- Unexpected traffic drop while removing BGP flowspec v4 and v6 in one commit PR1807693
- MX platforms with some MPCs could run into cm_error during ungraceful SIB or Peer-FPC power off event or due to bad fabric links PR1807812
- A route stuck in (Delete Hidden Ext) state forever due to BMP. PR1807892
- [MX] daemon.err rshd[618008]: Second port outside reserved range. PR1807939
- The IPsec tunnel traffic is dropped after ipsec tunnel soft reset on MX platforms PR1808207
- Openconfig data type value is streaming in gnmi update as float_val instead of bytes_val PR1808259
- CPU utilization of the rpd process stays high on all Junos and Junos OS Evolved platforms PR1808463
- The error message "sysctl kern.corefile not supported" is seen for multiple daemons during daemon initialisation PR1808481
- Traffic loss occurs if persistent link error is seen on a fabric plane to PFE, after restarting or rebooting another FPC in a different slot PR1808923
- On Junos MX204 platform and platforms with MPC7E/8E/9E, JNP10K-LC2101, JNP10003-LC2103, JNP10K-LC480 line cards, the interface goes down when re-initialisation issue occurs, causing 'Avago SERDES' EA (Eagle ASIC) chip crash PR1809306

- Ethernet interfaces configured with loopback option remains down after multiple iteration of line card boot is performed PR1809511
- FPC crash due to race condition on MX platforms with LC480 PR1809644
- The l2ald core is observed due to stale IFD entry PR1810013
- Error messages "dot1xd[xxxx]: %DAEMON-3-DOT1XD_MACSEC_GENCFG_ERROR: rtslib_gencfg operation failed ifd" seen after GRES PR1810563
- The rpd crash is observed due to the segmentation fault on Junos OS Evolved platforms PR1810866
- The rpd process crashes if the configuration changes rapidly when Tactical TE is enabled PR1811005
- PRPD flex routes with a translation tunnel (IPv4 to IPv6) type are not programmed if statistics is enabled. PR1811259
- In Junos MX platforms specifically MX2010 and MX2020 with SFB2 Fabric installed replacing MPC9E linecards with MPC6E linecards results in all SFB2 fabric get into check state and FPCs becomes destination error and offline PR1811474
- Intermittent SFB I2C failure Alarm and Alarm cleared after 3 polls of 5 seconds due to ZF0 VDD 0.75V intermittent access failure PR1811485
- XSTP reconverges after GRES (Graceful routing-engine switchover) with NSB (nonstop bridging) enabled if l2cpd in master is restarted before switchover PR1811511
- The LLDP neighborship does not recover on aggregated Ethernet interfaces. PR1811545
- ARP and ND entries are not in sync across the EVPN-VXLAN peers which leads to traffic drops PR1811556
- The process bbe-smgd crash will be observed in the Subscriber login/logout scenario PR1811787
- The rpd process crash is observed when there are catastrophic changes under the particular routing instance configuration PR1812009
- On MX2K, offline manually SFB2 or SFB3 or Plane to recover from a fabric link training failure, fabric mananger is not able to turn off the fabric links on a neighbor slot FPC PR1812046
- Persistent link error in one fabric plane towards some PFE could causes traffic blackholing from non-native LC PFE towards that remote PFE over all fabric planes PR1812276
- Persistent MAC getting stuck in the SRP state results in traffic loss in the EVPN-VxLAN scenario PR1812482
- PFCP Association stuck in disconnecting state for BNG CUPs platforms PR1812890
- Memory issue seen with syslog/log in firewall terms PR1813253

- Extensible Subscriber Services Manager (ESSM) sessions gets disconnected when PFE encounters an issue for any service or subscriber session PR1814017
- 'show system subscriber-management route summary' displays a negative gateway route count in the new master RE after UP-GRES PR1814125
- L2BSA sessions remain down when port messages from ANCP neighbor are dropped in a scaled scenario after ISSU followed by GRES PR1814300
- The dot1x authentication fails for VoIP traffic PR1814502
- Faulty MPC8 or MPC9 line cards can lead to spontaneous chassisd crash on certain Junos MX platforms PR1814801
- jnxSpSvcSetIfMemoryZone SNMP mib always returns 0 for service-set memory usage zone PR1814935
- JDI-RCT:M/Mx: after unsupported card is offlined during ISSU validation in MX router, fabric planes are stuck in check state PR1815125
- Premature graceful RE switchover causes traffic blackhole during software upgrade on PTX platforms with dual RE PR1815152
- The collector will see duplicate entries during the init sync of gNMI subscription on Junos and Junos Evolved platforms PR1815195
- The bbe-smgd crash is seen on MX platforms PR1815502
- Junos OS: SRX Series: Low privileged user able to access sensitive information on file system (CVE-2024-39527) PR1815751
- MAC addresses learnt on interfaces part of VLAN with MAC limiting by interface and "drop-and-log" action configured are cleared after VLAN description is changed PR1816049
- PFE core is observed due to PCIE link was down PR1816148
- XQSS_CMERROR errors will be seen which might disable PFE PR1816378
- JNP10K-LC480 Linecard fails to come online after restart due to CM Errors PR1816506
- Traffic blackholing will be observed in the l2circuit scenario when a non-active path is shut or disabled PR1816807
- IIC access error during commit operation cause false positive alarms in devices PR1816912
- Product annotation is missing for sensors on the MX, PTX, and EX92XX platforms PR1817967
- On Junos OS Evolved platforms, any new L2 functionality doesn't work when ELP configuration is not present on the connected device(s) PR1818022

- [LC480] STS LED may display incorrectly PR1818475
- Fan Tray Outer Fan running at over speed alarm is reporting after upgrade PR1818517
- Multiple BBE daemons getting killed automatically on MX platforms PR1818781
- The `preserve-nexthop-hierarchy` configuration configured with VPLS , brings down the Layer 3 protocol sessions running over the IRB interface PR1818978
- SRv6 to SRMPLS tunnel config changes cause rpd restart PR1819019
- The SNMP jnxFruRemoval/insertion trap OID is not being sent correctly when the FTC module or the fan tray module is inserted or removed PR1819263
- BMP gets stuck and does not send data to BMP collector PR1819305
- Switch port status is changed to unauthorized, when a supplicant client attempts to authenticate using 802.1X standard with EAP-TLS certificate PR1819462
- Multiple processes on both the REs are crashing. PR1820001
- The JTI/UDP export format prompts "gpb-sdm" as a possible completion on executing `set services analytics export-profile (profile name) format gpb-?` command. PR1820510
- Commit check does not display error while configuring `format gpb-gnmi` and `transport udp` for export-profile in Telemetry. PR1820774
- Traffic drop is seen in an EVPN multihoming scenario when mac-pinning is enabled. PR1820882
- The bbe-smgd daemon memory leak will be seen when ACI VLAN parsing fails. PR1821021
- The RADIUS attribute NAS-Port-Type is missing from Access-Request packets. PR1822101
- The PFE becomes inactive or disabled when running multicast in a video monitoring setup. PR1822738
- Few flows for BUM traffic gets dropped when a mix of MPC1-9 and MPC10 and above is used. PR1822793
- Aggregated ethernet interface flaps can be seen when IRB interface is activated or deactivated. PR1822911
- Authentication failure will be seen for routing protocols when MD5 is configured for routing protocols and PCEP on Junos OS Evolved platforms post reboot. PR1823220
- Interface will flap immediately on MX platform with MPC2 or MPC3 after FPC restart or router boot up. PR1823373
- Licensing usage is not set post reboot until there is an empty commit is done. PR1823449

- The jnxSubscriberPortTerminatedCounter shows incorrect values for interfaces. PR1824274
- New threshold values are set as LC4800 is not NEBS acoustic compliance. PR1824343
- The traffic is getting duplicated when VPLS to EVPN transition is performed. PR1824739
- On MX304 DHCP Vlan Creation Fails for EVPN VPWS when PIC0 is not installed. PR1825417
- The rpd crash is observed during upgrade or restart. PR1826194
- The error messages will be observed while configuring native sensor paths. PR1826196
- The subscribers get stuck post GRES switchover. PR1826324
- Even though installed the license to both primary and backup, Alarm LED might be lit with yellow on backup. PR1827641
- The pfemand crash will be observed when `clear bgp neighbor all` command is executed. PR1828017
- Potential Traffic will be seen on GRES/L2ALD Restart/GR due to Shadow INH Change. PR1828519
- In high-scale, high-load environments, the l2ald process might experience hangs during Apstra polling. PR1828741
- Inline NPTv6 is not working on classic firewall filters leading to packet processing errors. PR1828985
- The flowd process crashes in scaled scenario when subscribers exceed maximum session limit for NAPT44 on MX platforms with MX-SPC3. PR1829633
- Sourceport-ID comparison resulting in higher value for MPC7E compared to MPC5E for distributed PTP architecture. PR1830281
- Commit error on using more than 31 characters authentication-key-chain-name. PR1830395
- On Junos MX2020 platform with non-native LC, HSL2 'failed word alignment' error causes the fabric planes to go in check state. PR1830457
- The dcpfe crashes when ukern_trace handle buffer size is set to 10000. PR1830575
- FPC crash will occur when modifying or deleting a filter instance on Junos platforms. PR1830706
- Multiple flaps on BGP routes causing traffic sliently drops. PR1831421
- Telemetry streaming will not happen because the resource path is not valid. PR1831841
- The soft minor alarm 'QoS License(289) usage requires a license' is raised on the device. PR1832769
- Configuration Archival does not work using SFTP when using the mgmt_junos routing-instance on ACX5448. PR1833705

- The flowd process crash during TCP Packet Processing. PR1834248
- The RPD crashes after executing `show krt error-statistics errorno X`. PR1834859
- Fabric plane goes into check state and alarm is consistently seen along with traffic drop when ADC based line cards are restarted on certain MX platforms. PR1835860
- Subscriber's session created using the dynamic profile leads to rpd crash. PR1838354
- Traffic loss due to tunnel establishment failure in HA setup. PR1839090
- The Subscriber Sessions will stuck in the terminated state and the final accounting will be delayed PR1839200
- BMP soft assert due to counter reset by clear command PR1839288
- After performing ISSU on SRX4600, the SPM is no longer operational PR1839346
- RLT ifl remains down after RLT unit interface configuration is modified PR1840734
- PCP mapping fails for specific internal IPv4 addresses in DS-lite scenario PR1841231
- ISSU fail for the MPC2E/3E NG FPC result in FPC crash PR1841400
- Due to high bursty traffic, PIC on MX-SPC3 might go down. PR1841859
- An Enhancement to 'show ancp subscriber detail' command to display port-up/down timestamp and port-down cause PR1841954
- Unable to console to VNF using a non-root user from Juniper Device Manager PR1842451
- CFM session flaps continuously upon committing CFM inline mode and CFM sessions related configuration together PR1842542
- Inline IPsec tunnel traffic forwarding stops when destination IP prefix is moved from user-defined VRF (Virtual routing and forwarding) to default VRF or from default VRF to user-defined VRF PR1843098
- Traffic blockage observed with SFP-100BASE-BX10 optics in EX4400-48F PR1843585
- vlan tagging in Q-in-Q is not handled correctly over EVPN-VxLAN PR1843817
- Memory leak is seen with rpd task blocks "nhlib_nexthops_004" PR1844160
- Stale MAC-IP entries are not cleared in an EVPN-VXLAN scenario when encapsulate-inner-vlan or decapsulate-accept-inner-vlan or both knobs are present PR1844623
- High heap memory caused MX-SPC3 PIC to go offline PR1844731

- Packet duplication and flooding issues are seen when vpls bridge domain is configured on an aggregated Ethernet and label-switched interface across multiple line cards. PR1850604
- Unnecessary trace log files related to licenses are generated PR1845079
- Memory leaks are seen in bbe-statsd process. PR1852532
- Interface not added back to AE bundle with multiple changes in single commit PR1845370
- Incorrect warning message is seen post hyper-mode config change and mismatch of hyper-mode between FPC and RE impacts performance PR1845497
- Some ports take longer than others to come back online when multiple ports experience simultaneous flap PR1847378
- Core being generated for some processes while using license feature PR1848160
- Routing-services enabled on PPPoE dynamic profile causes subscriber login failure for new subscribers PR1848887
- Configuring BGP rib-sharding and generate route will cause rpd process to crash PR1848971
- The bbe-statsd process crash due to malformed PFE packets PR1849377
- FPC crash upon change of tunnel-services bandwidth PR1849552
- PR 1850604

  Packet duplication and flooding issues are seen when vpls bridge domain is configured on an aggregated Ethernet and label-switched interface across multiple line cards. PR1850604
- When BGP RIB Sharding is enabled, new BGP group/peer added gets stuck at Flags: (Sync InboundConvergencePending) PR1850620
- EVPN protocol configuration through CLI is not allowed on device PR1852905
- Router flag is not getting set in Neighbor Advertisement message PR1853868
- Devices fail to obtain an IP address when DHCP Security Option 82 is enabled. PR1854253
- IPv4 Frameroutes with prefix length of less than /32 do not get applied. PR1855891
- On MPC10/11, the traffic coming from any physical interface belonging to these MPCs will always take a fabric hop before forwarding to any physical link in egress. As a result despite locality bias feature being configured, the input traffic on that physical interface will still end up showing increase in the fabric statistics count. PR1857225

High Availability (HA) and Resiliency

- OSPF neighbours go down due to link flapping after NSR switchover on Junos OS Evolved platforms with IPSEC configuration PR1848313

Infrastructure

- Core dump capture failure during PeerStruck verification at medium threshold PR1816376

Interfaces and Chassis

- The LFM session flaps will be observed at random PR1811734
- After Routing Engine switchover the VRRP master and backup router will start functioning as master routers PR1822867
- The jpppd process will crash when subscribers frequently login and logout. PR1854387

Intrusion Detection and Prevention (IDP)

- Not able to update IDP signature DB when using Proxy server PR1822319
- Memory leak will be observed on all SRX platforms when IDP is configured PR1826377

J-Web

- Unable to load J-Web after upgrading SRX when time zone is set to GMT+x or GMT-x. PR1851362

Layer 2 Features

- VPLS traffic will be impacted when routing-engine switchover happens due to master routing-engine reboot in NSR scenario PR1793342

- RPD process terminates abnormally on MX480/MX10008 platforms by misconfiguration involving both BGP VPLS and LDP VPLS PR1813574

Layer 2 Ethernet Services

- After L2 failover, client receives DHCP attributes from the main pool configured instead of the linked pool and linked address-assignment pool name is not synced to DHCP binding on backup BNG having ALQ in BBE subscriber management scenario PR1799888
- The client session is logging out as DHCP renewal is not successful PR1801142
- jdhcpd cores when 'show dhcpv6 server binding' command is executed PR1816995
- DHCP asymmetric-lease-time is slow processing large scale requests to terminate 64K subscribers. PR1817227
- jdhcpd core dumps may be seen on ALQ setups when subscriber synchronization is done PR1818919
- JUNOS_REG:EX4650-48Y:ZTPv6:Failed to reconnect to device as unable to load configuration to device via shelscript from ztp server PR1822178
- DHCP ALQ process crashes to recover from memory leak. PR1825998
- DHCP relay option "allow-server-change" does not work as expected in trusted server group when roaming between access points PR1833148
- DHCPv6 BLQ not working as expected PR1839348

MPLS

- The rpd process crashes with LDP entropy-label policy configuration with "from instance (routing-instance-name)" PR1812545
- LSP keep retrying over the transit router marked as "overload" resulting in traffic drops or using the suboptimal path for the LSP PR1814358
- MPLS LDP sessions are not established when container-lsp is configured with an already existing lsp-template PR1817712
- LSP re-optimization issue has been observed PR1819948

- The detour path is not coming up when the detour hop limit is set to 255 PR1820893
- Bypass re-optimisation not taking SRLG or fate-sharing into account when protected link is down PR1823215
- Detours not coming up when link-protection is turned-off while interoperating with ZTE device PR1833448
- In a scenario involving NG-MVPN and point-to-multipoint LDP LSP the LDP point-to-multipoint FEC may remain in an inactive state on the PE after uplink interfaces flap PR1835938
- mgd timeout communicating with routing daemon rpd for 30 minutes during RSVP MBB event PR1837770
- The rpd crash is observed when "expand-loose-hop" knob is configured and rpd is undergoing graceful restart PR1840543
- RSVP authentication check fails if the length of the authentication-key is sixteen characters PR1850130
- Traffic loss will be observed when container-LSP with in-place-lsp-bandwidth-update configured. PR1857867

Network Address Translation (NAT)

- Commit error is observed on Junos platforms with MS-MPC or SPC3 when last octet of source-ip of jflow-log collector is above 223 PR1817417

Network Management and Monitoring

- The lo0 interface entries are missing from Junos 'ipNetToPhysicalTable' walk output PR1807176
- The "snmp packet-size (size)" command not working for SNMPv3 PR1817865

Platform and Infrastructure

- IP routes can get added to a deleted routing table PR1801129

- Multiple Products: RADIUS protocol susceptible to forgery attacks (Blast-RADIUS) (CVE-2024-3596) PR1802329
- 500 concurrent probes supported on Junos TVP platforms instead of standard 2000 probes for other Junos Platforms PR1808361
- Few error messages will be seen while deleting multiple EVPN Routing Instances. PR1808643
- Traffic drop is observed after any add/change/delete event on IRB interfaces inside a VPLS deployment PR1814521
- Console login fails when authentication-order is configured under 'system services' hierarchy on all Junos platforms PR1826666
- An authentication failure occurs when the TACACS+ server detects an error in sending authentication response PR1829031
- Traffic drops after link flap on active-active ESI setup with MAC pinning enabled PR1846365

Routing Policy and Firewall Filters

- Performance degrades when learning BGP routes with communities PR1795263
- OSPF neighbourship with IPsec authentication goes down after RE switchover PR1807830
- Firewalld process crashes when port range optimization parameter is configured with a value greater than 255 PR1815533
- Commit delay will be observed when the configuration is changed for the logical system PR1832853
- Static route validation fails when using an interface-route leaked with rib-groups using to rib as matching condition under rib-groups import-policy. PR1849500

Routing Protocols

- Memory leak in rpd due to deactivation and activation of routing-instances, interfaces and protocols PR1761191
- Leaked routes via BGP rib-group remains in hidden state even though "loops" is configured with any value greater than one PR1771344

- BGP OutQ counter of one of the BGP peers gets stuck after system reboot/restart routing/clear bgp neighbor PR1788543
- BGP routes may not get advertised when always-wait-for-krt-drain is configured with BGP sharding PR1793714
- Junos OS and Junos OS Evolved: Receipt of a large RPKI-RTR PDU packet can cause rpd to crash (CVE-2024-39543) PR1803120
- The CLI "show igmp snooping membership" does not list "instance" in its option PR1804715
- Junos OS and Junos OS Evolved: On SRv6 enabled devices, an attacker sending a malformed BGP update can cause the rpd to crash (CVE-2025-21593) PR1806694
- BGP backup routes are installed as primary routes after enabling 'protect core' feature PR1807037
- Interface and protocol flaps is observed when BFD authentication is enabled PR1807182
- BGP multipath selects wrong interface with "Multiple Single-Hop EBGP sessions on different links using the same IPv6 Link-Local Address" PR1807504
- Junos OS and Junos OS Evolved: When BGP traceoptions is enabled, receipt of specially crafted BGP packet causes RPD crash (CVE-2024-39525) PR1807533
- The rpd crash is observed for the leaked ISIS SRv6 locator route holding a stale pointer PR1808185
- BGP routes with next hops as link-local address are not installed PR1810617
- An interface with a lower MTU size is causing a rpd crash PR1810993
- Improper maximum value for limit-bandwidth of policy-statement PR1811862
- The rpd process crash is observed when the label received exceeds the configured maximum-labels 16 PR1812124
- The rpd process crash is observed when policy condition is applied to the route with a next-hop interface having nonzero logical unit PR1812844
- No new MoFRR back up path selected after changing the metric of back up PR1812857
- "snmp-options backward-traps-only-from-established" for logical-system doesn't work properly. PR1813048
- Local repair does not happen if BFD is configured on MX platforms with MPC7E line card PR1813841
- Incorrect counting of vrf-scale numbers for license warnings will be seen on all platforms PR1814012

- Junos OS and Junos OS Evolved: With BGP traceoptions enabled, receipt of specifically malformed BGP update causes RPD crash (CVE-2024-39515) PR1814083
- Junos OS and Junos OS Evolved: With certain BGP options enabled, receipt of specifically malformed BGP update causes RPD crash (CVE-2024-39516) PR1815222
- Junos OS: Multiple vulnerabilities resolved in OpenSSL (CVE-2024-4741, CVE-2024-2511) PR1815253
- The rpd crashes when stale label entry keeps increasing when knob stale-labels-holddown-period is configured PR1817834
- BGP-LU Label is incorrect after convergence PR1818545
- PIM Prune is not sent to upstream PR1819741
- Junos OS and Junos OS Evolved: When BGP traceoptions are configured, receipt of malformed BGP packets causes RPD to crash (CVE-2025-21598) PR1821241
- Junos OS and Junos OS Evolved: With certain BGP options enabled, receipt of specifically malformed BGP update causes RPD crash (CVE-2025-21600) PR1823612
- Unexpected behaviour after BGP sessions reset for catastrophic BGP configuration changes PR1826685
- Traffic impact due to BGP route stuck in hidden state PR1826686
- OSPF LSA flooding is impacted after database recovers from 'ignore' state when 'database-protection' is triggered PR1827435
- Memory leak can observed in SRv6 setup with TILFA enabled for SRv6 PR1828209
- Junos OS and Junos OS Evolved: Receipt of specially crafted BGP update packet causes RPD crash (CVE-2025-21602) PR1828380
- ISIS adjacency part of an igp-instance gets stuck in 'Initializing' state after the rpd restart PR1830989
- The 'overload advertise-high-metrics' does not work after the graceful restart for ISIS PR1837289
- BGP import policy does not process the next-hop statement PR1839318
- Configuration check-out fails when applying "inet6.0 static route" with qualified-next-hop and interface settings PR1839631
- The rpd crash after enabling ISIS with authentication keychain PR1839917
- Traffic drop is seen after GRES on ISIS peer PR1841108

- RPD process crash observed with dynamic tunnel configuration with overlap in destination networks under APP based and NHB mode and rollback PR1842654
- MVPN traffic does not recover after clearing forwarding-cache PR1845087
- BGP stops advertising VPN routes to EBGP peer if static route-target-filter as local is configured PR1845169
- The S-BFD responder session cannot be distributed to PFE and failing S-BFD session to establish PR1846448

Services Applications

- Radius-flow-tap Lawful Intercept DTCP ADD request is not accepting port ID and constantly using port 47355. PR1839617

Subscriber Access Management

- Address preservation for delegated prefixes does not work for subscribers in VRF PR1777967
- authd process crashes when radius-server-name is configured PR1818321
- The authd process crash is seen when subscriber management is enabled PR1826901

User Interface and Configuration

- XML namespace string in rpc-reply tag for system-uptime-information was changed to represent the full version name. PR1842868

VPNs

- MPLS LSP tied to an l2circuit is not honoring the configured transport class PR1834625

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading to Release 24.2R1

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.

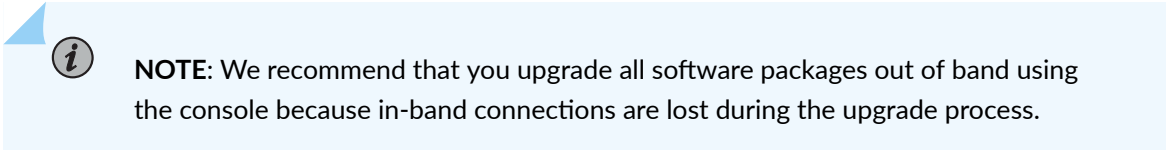
Procedure to Upgrade to Junos OS

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-x86-32-20.4R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-20.4R1.9-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-x86-32-20.4R1.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-20.4R1.9-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 24.2R1, 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.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

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

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

Table 4: EOL and EEOL Releases

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

For more information about 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.

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 24.2R1

To downgrade from Release 24.2R1 to another supported release, follow the procedure for upgrading, but replace the 24.2R1 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for NFX Series

IN THIS SECTION

What's New

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

What's Changed

There are no changes in behavior and syntax in this release for NFX Series devices.

Known Limitations

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

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

Open Issues

IN THIS SECTION

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

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

General Routing

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

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

- On the NFX350 devices, `srxpfe core` is seen.PR1792616.

High Availability (HA) and Resiliency

- When high availability (HA) is enabled and fabric links are configured on NFX devices (NFX150, NFX250 and NFX350 with nfx-3 software package), the fabric link monitored status is displayed as `Down` leading to an `FL` status.PR1794559

Interfaces

- On the NFX350 device, even though the ethernet cable is physically plugged in and the `show interface command`displays Front panel LED status as `up`, the front panel LED is not ONPR1702799

Resolved Issues

IN THIS SECTION

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

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

Interfaces

- Starting in Junos OS Release 24.2R1 release, when you run the command `show chassis alarm` on NFX 350 devices, the output displays `Major TSensor 3:Coretemp Access Failed` due to swapping of the symlinks of hwmon0 and hwmon1.PR1769699

Network Address Translation

- On the NFX devices when the NAT port number or the IP address of the peer device located behind a Network address translation (NAT) device is changed, the next Dead Peer Detection (DPD) or rekey process fails to update the port number in the existing tunnel NAT Traversal (NAT-T) flow session. The failure to update the port-number happens if the DPD is configured as `always-send`. This condition leads to communication failure over the Internet Protocol Security (IPsec) tunnel.

PR1776216

VNF

- On the NFX platforms, the `pfe` (Packet Forwarding Engine) process crashes when configured with custom mode templates like flex mode or any other custom mode due to memory exhaustion. PR1776815

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

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

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

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

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

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

Table 5: EOL and EEOL Releases

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

For more information about 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.

Basic Procedure for Upgrading to Release 24.2

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

NOTE: The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the

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

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

To download and install Junos OS Release 24.2R1:

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

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

2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the **Software** tab.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list to the right of the Download Software page.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the device or to your internal software distribution site.
10. Install the new package on the device.

Junos OS Release Notes for QFX Series

IN THIS SECTION

What's New

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

What's Changed

IN THIS SECTION

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

NOTE: For all QFX5110 models, the standard name of the image has been changed from "5e" to "5x." As follows:

Old format: jinstall-host-qfx-5e-

New format: jinstall-host-qfx-5x-

The new format is in effect starting with Junos OS 24.2R1 and will be used for all subsequent mainline Junos OS releases. No maintenance or service releases for release trains prior to 24.2 will implement the change.

Routing Protocols

- **MLD snooping proxy and l2-querier source-address (ACX7024, ACX7100-32C, EX4400-24MP, PTX10001-36MR, QFX5120-32C, and QFX5130-32CD)**— The `source-address` configured for `proxy` and `l2-querier` under the `mld-snooping` hierarchy should be an IPv6 link-local address in the range of fe80::/64. The CLI help text has been updated to "Source IPv6 link local address to use for proxy/L2 querier". In earlier releases, the CLI help text read, "Source IP address to use for proxy/L2 querier."

  [See source-address.]

User Interface and Configuration

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the `Hostname` field first instead of last. The `show version` command output includes the `Family` field. The `Family` field identifies the device family under which the device is categorized, for example, `junos`, `junos-es`, `junos-ex`, or `junos-qfx`.

  [See show system information and show version.]

Known Limitations

There are no known limitations in hardware or software 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.

Open Issues

IN THIS SECTION

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

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

General Routing

- Misleading syslog message "L2CKT/L2VPN acquiring primaryship for primary" though no VPN/ L2CKT configured on the router. PR1105459
- The 4x25G channelized interfaces are not coming up after optics hot swap. PR1719758
- Channelized interfaces leds are not properly represented in `show chassis led`. PR1720502
- In a QFX51200-48YM-8C VC setup, after a a primaryship switch over fan tray of linecard might not be displayed in show chassis hardware and show chassis environment. There is no functional impact. PR1758400
- QFX5210: dcpfe core seen at __kernel_vsyscall,tvp_watchdog,dcbcm_driver_read32,soc_dcbcm_ipoll_check,cpu_sched_update_timers. PR1790234
- Due to a the disk failure reboot support was not added for dual disk scenario, hence system was not booting in case of disk failure on sdb (the other disk) on QFX platform. PR1800862
- On Junos QFX5100 and EX4600 Platforms, high storage Utilisation is observed in /var/log due to uncompressed UKERN_GBL.log file. This can lead to low storage warnings and potential write errors for other system logs during that period. PR1804090

- On all Junos QFX5000 platforms, traffic loss happens and the layer 3 interface cannot be deleted when many routes use the same layer 3 interface. QFX5000 is encapsulating the packets with the wrong DMAC(destination MAC) and VNID(virtual network identifier) for a few IP addresses after disabling the interface. PR1808550
- The traffic is still getting forwarded to all the interfaces mapped with concerned VLAN even after `unknown-unicast-forwarding` configuration statement is enabled on all Junos QFX10000 platforms, but it is allowed to be configured, so the command is disabled to avoid misconfiguration. PR1810120
- On all Junos QFX5000 platforms, with ECMP (Equal Cost Multi Path) configured, when there is any routing protocol change (like ISIS cost metric change), the protocol traffic on the network is dropped. PR1823601
- The PTX10008, PTX10002-60C, or QFX10002-60C platforms might not send back ICMPv4/v6 reply packets properly due to defects leading to misprogramming of hardware. Ping with v4/v6 from another device to the PTX10008, PTX10002-60C, or QFX10002-60C platform will fail. PR1827286

High Availability (HA) and Resiliency

- Graceful Routing Engine Switchover (GRES) not supporting the configuration of a private route, such as fxp0 , when imported into a non-default instance or logical system. Please see KB https:// kb.juniper.net/InfoCenter/index?page=content & id=KB26616 resolution rib policy is required to apply as a work-around. PR1754351

Junos XML API and Scripting

- On all Junos platforms where snapshot is supported, when a device is rebooted from recovery mode it fails to commit configuration due to problems with slax import and device might go into amnesiac mode due commit fail. PR1717425

Routing Protocols

- On all Junos and Junos OS Evolved platforms, multiple simultaneous Command Line Interface (CLI) sessions will lead to high Management Daemon (mgd) CPU utilization, impacting the device's reachability over the loopback interface from IS-IS nodes. PR1749850

User Interface and Configuration

- ZTP upgrade in dual RE fails if the image name has special characters. PR1851232

Resolved Issues

IN THIS SECTION

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

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

General Routing

- JDI_REG::QFX5200:: After ISSU upgrade, device is hanged and not able to perform any operations until USB recovery done on device. PR1703229
- JUNOS_REG: QFX5110-48S : "mge" interface is going down after performing soft OIR. PR1757704
- 100G optics set to CAUI4 on Junos QFX5200-32C platforms. PR1758868
- Untagged traffic gets dropped when 'native-vlan-id' and 'vlan-id-list' are configured together under same interface. PR1771445
- 100G optics settings to CAUI4 on Junos QFX5120-48T platforms. PR1773567
- Temporary traffic flooding when root port flaps in all flavours of STP. PR1775171

- Interface flap occurring unexpectedly on Junos QFX platforms. PR1777336
- The fxpc process crash and the device reboots after deleting Aggregated Ethernet (AE) Interface along with its associated physical interface and then applying new interface configuration on the associated physical interface in an EVPN-VXLAN scenario. PR1783397
- QFX5000 : The pps rate for egress interface becomes zero after removing one of VCP ports. PR1786119
- The port class is not captured in cint trace output for individual ports. PR1786399
- Nexthop is not getting uninstalled from FPC and is throwing errors causing traffic drop. PR1789507
- Layer 3 multicast traffic gets dropped when a BD is configured with IRB as the source interface. PR1793772
- The 100G VCP will go down upon restarting or upgrading the device. PR1796218
- On Junos QFX5000, EX4100, EX4300, EX4400 and EX4650, Type 5 tunnel traffic loss observed when all IRB interfaces are deleted. PR1798684
- Traffic drops are observed in the EVPN-VXLAN environment having IPv4 and IPv6 address configured in underlay. PR1798887
- Auto-channelization is showing inconsistent behaviour on QFX platforms when there is fault on the channels. PR1799073
- Traffic drop is observed when an SP style port is added to an existing vlan lag interface. PR1801217
- The default port behaviour is not working as expected after deleting VOIP (Voice over IP) configuration on an access interface. PR1802455
- VRRP Gateway IP Unreachability. PR1802615
- The dcpfe process will crash in an EVPN-VxLAN scenario due to stale entries in PFE. PR1804628
- When VC-mode is set to HGOE and converting port type from vc-port to network port, traffic loss is observed. PR1806262
- VRRP multicast packets coming from external hosts connected to the EVPN-VXLAN fabric might get duplicated on QFX10000 platforms. PR1808040
- The dcpfe process crash is seen in case of inline sampling. PR1808041
- The Layer 3 Multicast traffic will be dropped in an OISM scenario when an egress interface is configured with native-vlan /Access mode. PR1808816
- IPv6 NS packets not forwarded to access port due to VXLAN snoop entry. PR1810169

- Link wont come up on bounce of fec91 on QFX5120 platform. PR1810740
- Multiple services and protocols does not work on the backup member with 100G port used as VC interconnect port on QFX5110-48S. PR1811701
- Persistent MAC getting stuck in the SRP state results in traffic loss in the EVPN-VxLAN scenario. PR1812482
- IPv6 transit traffic is getting impacted in a rare scenario with Longest Prefix Match (LPM) profile configuration. PR1813250
- Configuring Multiple vlan-id-list on an interface will not program all the VLANs on QFX5110 devices. PR1813454
- The traffic loss is observed if both Layer 3 unicast and VTEP next hop are used to reach same destination. PR1814387
- ARP resolution issues might happen when VxLAN and non-VxLAN are both configured on the same ifd but different ifl. PR1815250
- MAC addresses learnt on interfaces part of VLAN with MAC limiting by interface and "drop-and-log" action configured are cleared after VLAN description is changed. PR1816049
- DHCP snooping issue Observed on Access Ports with IRB and VXLAN configuration. PR1816445
- EVO(EVPN Fabric): DHCP packets are getting relayed even after deleting the dhcp relay configuration from the leaf. PR1817061
- On QFX10002-60C, after upgrading or rebooting, random failures may occur on 10G links. PR1818082
- On Junos QFX5000 Series platforms multicast traffic impact is observed after device reboot. PR1818740
- An error log message is seen for every DHCP transaction. PR1818909
- Traffic received over the Type-5 tunnel is getting dropped due to the network port not having the correct flags set in the pure Type-5 EVPN-VXLAN scenario. PR1819073
- Egress-link-protection in combination with IGMP/MLD snooping breaks snooping functionality. PR1820318
- Traffic drop is seen in an EVPN multihoming scenario when mac-pinning is enabled. PR1820882
- L2TP Processing Issue on EX and QFX Platforms with Tagged CDP VTP and UDLD frames. PR1821012

- Traffic loss is seen in an EVPN-VXLAN scenario when an Layer 2 underlay interface is configured using a service provider style. PR1821549
- QFX : dfw ERROR is seen whenever collecting RSI. PR1823280
- In virtual-chassis after routing-engine switchover traffic of type 5 routes of EVPN-VXLAN are not getting forwarded. PR1823764
- The SFP 10GBASE-T part No. 740-083295 on platforms running Junos is unable to detect a linkdown. PR1823771
- Restricted Proxy ARP feature does not work as expected. PR1824023
- Rebooting one linecard or FPC will cause the virtual-chassis on the EX4000 and QFX5000 devices to forward traffic in backup RTG interface. PR1824750
- IPv6 PTP packets are getting dropped resulting in PTP synchronization issues. PR1827299
- ARP not learned on Switch Leading to Traffic Drop in EVPN-VXLAN Setup. PR1827648
- FPC crash will occur when modifying or deleting a filter instance on Junos platforms. PR1830706
- Junos QFX5000 configured with l2circuit stops forwarding traffic on IFD with vlan-ccc encapsulation subunit when deleting or adding one of the IFLs. PR1830828
- The "unknown-unicast-forwarding" feature is allowed to be configured even though it is not supported for the target platform. PR1831498
- VRRP fails on 802.1Q VLAN Layer 3 logical interface on QFX10002-60C. PR1834429
- VXLAN overlay traffic is tagged with a native VLAN when an underlay NNI is configured with a native VLAN on all Junos QFX5000 platforms. PR1834627
- On all Junos QFX5000 platforms the next hop for WECMP (Weighted Equal Cost MultiPath) is not programmed in PFE (Packet Forwarding Engine) properly. PR1838623
- Delay in GBP installation in an EVPN-VXLAN scenario. PR1839916
- The VXLAN ARP packets goes to the ARP queue 34 after disabling ARP suppression. PR1840251
- QFX5210/AS7816 lpm ip route install failed due to table full unit 0. PR1841913
- Traffic drops are observed in the EVPN-VxLAN scenario due to VPLAG flaps. PR1842475
- VLAN tagging in Q-in-Q is not handled correctly over EVPN-VxLAN. PR1843817
- Unnecessary trace log files related to licenses are generated. PR1845079
- Core being generated for some processes while using license feature. PR1848160

EVPN

- VXLAN/EVPN ip-address for mac-address in forwarding table in hold state. PR1802464
- The MAC pinning functionality is not working on QFX platforms. PR1806416
- Error messages are observed after performing a VLAN name change with EVPN configuration. PR1806660
- EVPN-VXLAN Egress Link Protection Incompatibility with STP Affecting FRR Performance. PR1815823
- Command `set protocols evpn designated-forwarder-preference-least` not working correctly. PR1823351
- Continuous kernel log messages are observed once the EVPN-VXLAN fabric is up. PR1826772

Layer 2 Ethernet Services

- The AE interface flaps when the force-up configuration statement is enabled and child link also flaps. PR1827241
- Unable to assign an IP address on management interface with DHCP configuration even if DHCP is bound after a power cycle. PR1854827

Platform and Infrastructure

- Multiple Products: RADIUS protocol susceptible to forgery attacks (Blast-RADIUS) (CVE-2024-3596). PR1802329
- Console login fails when authentication-order is configured under 'system services' hierarchy on all Junos platforms. PR1826666

Routing Protocols

- The CLI `show igmp snooping membership` does not list "instance" in its option PR1804715
- Junos OS: Multiple vulnerabilities resolved in OpenSSL (CVE-2024-4741, CVE-2024-2511). PR1815253

- Configuration check-out fails when applying "inet6.0 static route" with qualified-next-hop and interface settings. PR1839631

Virtual Chassis

- QFX5120 Virtual Chassis (VC) drops Address Resolution Protocol(ARP) packets from remote leaf. PR1773425

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.

NOTE: For all QFX5110 models, the standard name of the image has been changed from "5e" to "5x." As follows:

Old format: jinstall-host-qfx-5e-

New format: jinstall-host-qfx-5x-

The new format is in effect starting with Junos OS 24.2R1 and will be used for all subsequent mainline Junos OS releases. No maintenance or service releases for release trains prior to 24.2 will implement the change.

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

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 24.2 release.

   An Alert box appears.

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

   A login screen appears.

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

7. Download the software to a local host.

8. Copy the software to the device or to your internal software distribution site.

9. Install the new jinstall package on the device.

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

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

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-24.2-R1.n-secure-signed.tgz reboot
```

Replace *source* with one of the following values:

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 24.2 `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-x86-64-20.4R1.9.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-
x86-64-20.4R1.9.tgz
```

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

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

Installing the Software on QFX10002 Switches

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

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

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

For example:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-f-x86-64-20.4R1.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-x86-64-20.4R1.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-
x86-64-20.4R1.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-
x86-64-20.4R1.n-secure-signed.tgz
```

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

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

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

NOTE: You must reboot to load the new installation of Junos OS on the switch. To abort the installation, do not reboot your system. Instead, finish the installation and then issue the `request system software delete jinstall` *<package-name>* command. This is your last chance to stop the installation.

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

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

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

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

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

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

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

```
user@switch> show chassis routing-engine
Routing Engine status:
```

```
  Slot 0:
    Current state                  Master
    Election priority              Master (default)

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

Performing a Unified ISSU

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

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

Perform the following tasks:

- Preparing the Switch for Software Installation
- Upgrading the Software Using Unified ISSU

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

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

  To verify that nonstop active routing is enabled:

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

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

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

- Enable nonstop bridging (NSB). See Configuring Nonstop Bridging on EX Series Switches for information on how to enable it.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the `request system snapshot` command.

Upgrading the Software Using Unified ISSU

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

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in Installing Software Packages on QFX Series Devices.
2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:
   - On the switch, enter:

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

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

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

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

```
warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get lost!
ISSU: Validating Image
ISSU: Preparing Backup RE
Prepare for ISSU
ISSU: Backup RE Prepare Done
Extracting jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz ...
Install jinstall-host-qfx-5-f-x86-64-19.2R1.n-secure-signed.tgz completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status                  Reason
  FPC 0          Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff
```

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

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

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

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

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

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

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

Table 6: EOL and EEOL Releases

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

For more information about 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 SRX Series Firewalls

IN THIS SECTION

What's New

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

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series Firewalls.

Application Security

- **Application Signatures Package (SRX Series Firewalls and vSRX)**—The `show services application-identification status` command output displayed incorrect date for application package version release date. The command output displays the release date of the initial installed application signature package. Subsequent installations of newer versions do not update the release date of the signature package. The release date is only updated correctly when installing a signature package that has changes in PB version/Engine version compared to the currently installed ones.

  Starting in Junos OS Release 24.2 onwards, the command output shows the correct date.

  See show services application-identification status.

- **Deprecation of 3DES-CBC ciphers (SRX Series Firewalls and vSRX)**—Support for the following ciphers is deprecated:

  - RSA-3DES-EDE-CBC-SHA
  - ECDHE-ECDSA-3DES-EDE-CBC-SHA

  The options to configure these ciphers are not available at the [*edit system services ssh*] hierarchy.

Interfaces

- **Autonegotiation in xe ports (SRX380)**—Starting in Junos Release 24.2R2, autonegotiation is disabled by default on all the four xe ports of SRX380 Firewalls. It is recommended to disable the autonegotiation at the remote end devices. To change the autonegotiation default recommended behavior, use the `set interfaces xe-x/y/z gigether-options auto-negotiation` command.

- Starting in Junos OS Release 24.2R1, when you run the run `show lldp local-information interface <interface-name> | display xml` command, the output is displayed under the `lldp-local-info` root tag and in the `lldp-local-interface-info` container tag. When you run the run `show lldp local-information interface | display xml` command, the `lldp-tlv-filter` and `lldp-tlv-select` information are displayed under the `lldp-local-interface-info` container tag in the output.

- **Disable keyword removal (SRX300, SRX320, SERX340, SRX345, SRX380, SRX550, SRX550M)**–The `watchdog disable` option has been removed from the `set system processes` command. You cannot configure `watchdog disable` anymore.

- **Increased limit for number of concurrent probes for real-time performance monitoring (SRX1500, SRX1600, and SRX2300, and SRX4300)**–We have increased the number of concurrent probes allowed for real-time performance monitoring (RPM) to 2000 from the previous limit of 500. [See probe-limit.]

Junos OS API and Scripting

- **Changes to the XML output for ping RPCs (MX480)**—We've updated the `junos-rpc-ping` YANG module and the corresponding Junos XML RPCs to ensure that the RPC XML output conforms to the YANG schema. As a result, we changed the XML output for the following ping RPCs:
  - `<ping>`—The XML output emits `<ping-error-message>` and `<ping-warning-message>` tags instead of `<xnm:error>` and `<xnm:warning>` tags.
  - `<request-ping-ce-ip>`—The XML output is enclosed in an `<lsping-results>` root element.
  - `<request-ping-ethernet>`—
    - The `<ethping-results>` root tag includes a `<cfm-loopback-reply-entry>` or `<cfm-loopback-reply-entry-rapid>` tag for each received response. In earlier releases, a single tag enclosed all responses.
    - The XML output includes only application specific error tags and omits `<xnm:error>` tags.
    - The `<cfm-loopback-reply-entry-rapid>` tag is now reflected in the YANG schema.
  - `<request-ping-overlay>`—The `<ping-overlay-results>` element includes a new child tag `<hash-udp-src-port>`.

PKI

- **Enhancement to fix output with Junos PyEz for duplicate keys in PKI (MX Series, SRX Series, EX Series)**—In earlier releases, though the CLI output displayed all the duplicate keys for the corresponding hash algorithms in PKI using `show security pki local-certificate detail | display json` command, for the same requested data, Junos PyEz displayed the last key only. Starting this release, the CLI output and the PyEz displays all the duplicate keys with the enhanced tags.
- **Certificate enrollment system logs (Junos)**—We've added system logs to notify if there is an SCEP and CMPv2 certificate failure. On SCEP certificate enrollment failure, you can see the PKID_SCEP_EE_CERT_ENROLL_FAIL message. On CMPv2 certificate enrollment failure, you can see the PKID_CMPV2_EE_CERT_ENROLL_FAIL message. See System Log Explorer.

User Interface and Configuration

- **The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX and vSRX)**—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version

emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

- **Access privileges for request support information command (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance` , `view` , and `view-configuration` can execute request support information command.

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the `Hostname` field first instead of last. The `show version` command output includes the `Family` field. The `Family` field identifies the device family under which the device is categorized, for example, `junos`, `junos-es`, `junos-ex`, or `junos-qfx`.

  [See show system information and show version.]

VPNs

- **Enhancements to fix the digest option functionality for key pair generated with DSA and ECDSA (SRX Series and vSRX 3.0)**—In earlier releases, when you generated local self-signed certificates using sha-256 digest and DSA or ECDSA encryption using `request security pki generate-key-pair certificate-id` *`certificate-id-name`* `size` *`size`* `type (dsa | ecdsa)` and `request security pki local-certificate generate-self-signed certificate-id` *`certificate-id-name`* `digest sha-256 domain-name` *`domain-name`* `subject` *`subject-distinguished-name`* commands, the generated signature always used sha1 digest. Starting this release, the specified digest, sha-256, is used for the signature digest. You can verify using `show security pki local-certificate certificate-id` *`certificate-id-name`* `detail`

- **Enhancements to address error in generating RSA key pair with bigger key size (SRX Series)**–In earlier Junos OS releases, when you generate RSA key pair of size 4096 or greater, the command `request security pki generate-key-pair certificate-id` *`name`* `type rsa size 4096`, displays the error message `error: timeout communicating with pki-service daemon` sometimes when PKID takes more time to respond. Starting in Junos OS release 23.4R1, the command runs successfully without this error message.

- **Enhancements to the IKE configuration management commands in chassis cluster (SRX Series)**--In earlier Junos OS releases, in a chassis cluster mode, the following commands failed with the error message `error: IKE-Config-Management not responding to management requests` on the secondary node:

  - `show security ike statistics`
  - `show security ike sa ha-link-encryption`
  - `show security ipsec sa ha-link-encryption`

- `show security ipsec inactive-tunnels ha-link-encryption`
- `clear security ike sa ha-link-encryption`
- `clear security ipsec sa ha-link-encryption`

You should run these commands only on the primary node rather than the secondary node. Starting in Junos OS Release 23.4R1, you'll not see the error message as the secondary node has no output to display.

- **Enhancements to the help string description for the threshold and interval options for VPN monitoring options (SRX Series and vSRX 3.0)**–We've enhanced the help string description of the `threshold` and `interval` options available in the configuration statement `[set security ipsec vpn-monitor-options]` to include the default values. You'll see the following description with the default values:

```
user@host# set security ipsec vpn-monitor-options ?
Possible completions:
interval Monitor interval in seconds Default :10 (2..3600 seconds)
threshold Number of consecutive failures to determine connectivity Default :10 (1..65535)
```

[See ipsec (Security).]

- **Enhancements to the output of show security ipsec security-associations detail command (SRX Series and vSRX 3.0)**–We've enhanced the output of `show security ipsec security-associations detail` when you enable `vpn-monitor` at the `[edit security ipsec vpn vpn-name]` hierarchy level, when your firewall runs IPsec VPN services with the new iked process. The output displays `threshold` and `interval` values in the command output. Starting in Junos OS Release 23.4R1, you'll notice these changes.

  [See show security ipsec security-associations.]

- **Enhancements to address certificate validation failures after RG0 failover (SRX Series)**–Following RG0 failover in the chassis cluster, you may notice that the output of the command `show services advanced-anti-malware status` displays `Requesting server certificate validation` status due to CRL download failure on the secondary node before the failover. We've made enhancements to address the issue and you'll see the following changes:

  - If there's a repeated failure to download the CRL even after multiple retry attempts, you will notice the error message `PKID_CRL_DOWNLOAD_RETRY_FAILED: CRL download for the CA failed even after multiple retry attempts, Check CRL server connection` until the CRL downloads successfully.
  - When the cluster performs a failover from the secondary to the primary node, the PKI triggers a fresh CRL download on the new primary node, resulting in successful certificate verification.

- **Reauthentication frequency recommendation for IPsec VPN with PPK (SRX Series and vSRX 3.0)**—For IPsec VPN, including the Auto Discovery VPN (ADVPN), with post-quantum pre-shared key

(PPK) encryption, when the IKE security association is negotiated with the quantum keys, the iked process performs rekeying after 4 seconds to secure the channel. If you set the reauthentication frequency to 1, rekeying doesn't happen after 4 seconds. So we recommend you to set the reauthentication frequency to more than 1 as the first reauthentication count is used by the PPK default rekey.

[See Quantum Safe IPsec VPN.]

- Optimized dead peer detection for NAT-T (SRX Series Firewall and NFX Series)-When the NAT-T remote port changes, incoming Dead Peer Detection (DPD) from the peer device may create a new session, leading to session mismatches and traffic interruptions. To prevent this, you can enable optimized dead peer detection. Use the command set security ike gateway gateway-name dead-peer-detection optimized to ensure that any new session created during incoming DPD expires, and the existing tunnel NAT-T session is updated with the new port number, allowing traffic to resume. See Understanding NAT-T.

Known Limitations

IN THIS SECTION

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

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

- Feature for rst_sequence knob request SPU flow to keep having sequence number in the record, But, for sessions which has been offloaded, the packet is forwarded directly on NP, due to which SPU did not receive the packet. Also, the sequence number is not synced to the SPU session with the current design, and there is no mechanism to do it. That is why, this feature cannot be support on the

offloaded sessions. This is a design limitation when SOF is enabled. So, to use the feature of rst_sequence check we will need to disable the SOFPR1830053

Platform and 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
- This issue is caused because of the fact that peers-synchronize is configured, and master-password is configured to encrypt the config being sync'ed. However since there is no master-password configured on the peer device, the encrypted configuration cannot be decrypted (this is expected). This has not been supported from day-1, however a workaround can be done in order to get this to work. The workaround is to manually configure the same master password on the peer device manually. At a high level the problem is as follows: Consider there are two devices A and B in a peer-sync config 1. config on dev A contains secrets which need to be encrypted with the master password and synced with the device B 2. The master-password (juniper123+masterpassword) is configured on device A and the configuration is encrypted and written to /tmp/sync-peers.conf 3. The /tmp/sync-peers.conf is then synced to device B but device B does not have the same master-password configured which results in the config failing to decrypt. The master-password itself is not a part of the config-database. Additionally, it cannot be transmitted over an unencrypted HA Link, as this would lead to the master-password getting leaked. This is by design, and would be a security concern if it were to be transmitted across an unencrypted channel. Therefore, this work as designed. In order to work around this issue follow these steps: 1. configure the master-password on device B and commit the config 2. configure the same master-password on device A and commit the config and it should get sync'ed correctly.PR1805835
- An Authentication Bypass by Spoofing vulnerability in the RADIUS protocol of Juniper Networks Junos OS and Junos OS Evolved platforms allows an on-path attacker between a RADIUS server and a RADIUS client to bypass authentication when RADIUS authentication is in use. Please refer to https://supportportal.juniper.net/JSA88210 for more information.PR1850776

User Interface and Configuration

- On SRX300 series plaforms, when running BFD, performing CLI commands which have a long output and high impact on control plane CPU load, may cause a BFD flap. In such case, use the Dedicated BFD or Real-time BFD feature to avoid the impact.PR1657304

Open Issues

IN THIS SECTION

Learn about open issues in this release for SRX Series Firewalls.

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

Chassis Clustering

- With restart-chassis control command on SRX4200, SRX4700, and SRX5000 line of devices, BFD ICL will flap. PR1789245
- Performing an ISSU on an SRX1600 cluster from Junos OS release 24.2R2 to a supported release might generate SRXPFE core files, but the ISSU will successfully complete. PR1896182

Flow-Based and Packet-Based Processing

- When multicast traffic triggers a route resolution request for a pending session, and the route is subsequently resolved, a race condition may occur if that pending session is terminated by a different thread before processing can continue. This can result in a crash of the flowd (security forwarding process). However, the control plane remains online and unaffected.PR1859163

General Routing

- Additional logging has been added to the primry Routing Engine. This is to help narrow down the issue which chassisd process restarted unexpectedly at snmp_init_oids( ) function on the primary Routing Engine while booting up.PR1787608
- Right after rebooting one of SRX4600 at HA setup, CTL link might keep down.PR1802158
- On Junos SRX4100/SRX4200 platform, starting and stopping the "monitor traffic interface" or "tcpdump", causes VLAN tagged traffic to be dropped. While the "monitor traffic interface" or "tcpdump" is still running the traffic will function properly, but traffic will stop flowing when it is stopped. This issue only occurs on vlan-tagged interfaces.PR1808353
- On Junos SRX5600 and vSRX3 platforms while upgrading from an older JUNOS version to 22.4R3-S1 or 22.4R3-S2, the upgrade process can fail as the rpd crashes as part of validation process. This is seen if the router config has Multicast/Internet Group Management Protocol (IGMP) or Broadband Edge configuration.PR1810817
- MACSec is supported in routing mode but not in transparent mode.PR1812427
- On all SRX platforms except for SRX5k series platforms , when Secure or Explicit Web Proxy is configured, the flowd process crasches due to a race condition causing traffic outage.PR1813355
- On SRX1500 platform, large IP packets of size 1470 bytes or larger may be dropped when using ethernet-switching and trunk ports.PR1813536
- MNHA Conn State is going down after 48+ hours with some background traffic when MNHA ICL is configured with link-encryption PR1822662
- As per OpenSSH 9.0/9.0p1 release notes: "This release switches scp(1) from using the legacy scp/rcp protocol to using the SFTP protocol by default." In this case, since we are running OpenSSH 9.0 and above- OpenSSH_9.7p1 , this uses the "SFTP" protocol by default when scp command is invoked from shell. However, vSRX3.0 supports the "SCP" protocol by default when scp command is invoked. So to use the legacy "SCP" protocol from shell, please use the -O command line option For example: scp -O other options arguments Note: Incoming SCP connections from outside hosts that are running OpenSSH version 9.0/9.0p1 could fail since sftp-server is disabled by default in Junos OS . Hence, users should either use the -O option on remote host while initiating scp file transfer OR enable sftp-server in the Juniper configuration. To enable sftp-server in Juniper configuration, use the following hierarchy: "set system services ssh sftp-server"PR1827152
- On Junos SRX1600, SRX2300 and SRX4300 platforms, when MVRP (Multiple VLAN registration protocol) is enabled along with static vlans, the dynamic vlan learning and assignment doesn't work resulting in traffic loss for the impacted vlans. This issue is observed only when the interface is converted into routing mode and rolled back to switching mode.PR1839275

- On SRX3xx series configured with native-vlan-id, after upgrading an SRX3xx series device to Junos version 23.4R1 or higher, the native-vlan-id option disappears from the interface settings. If native-vlan-id was set before the upgrade, the device keeps the setting but it doesnt apply it to the interface. Trying to delete native-vlan-id causes a syntax error. The native-vlan-id feature doesn't work, and if a custom VLAN ID (other than 1) was used then traffic for that VLAN will be affected.PR1847366
- On SRX and MX platforms a rare occurrence issue causes a sudden reboot of the SPC3 (Services Processing Cards) in use leading to packet loss during the card offline period in the reboot process.PR1857890

J-Web

- On SRX4600, upgrades and downgrades will fail from J-Web with the error message: "Installation Progress failed at Receive Package File" from release 23.4 and above.PR1876075

Network Address Translation (NAT)

- The existing RSI misses out on few important information from NAT plugin, which can now be collected via a new RSI CLI command - "request support information security-components nat". This will provide more data and help in better debugging.PR1825372

Platform and Infrastructure

- On SRX5400/SRX5600/SRX5800 platforms, if vmcore is initiated for XLP PIC (Extreme Low Power Peripheral Interface Controller), vmcore process crashes.PR1811765
- An Authentication Bypass by Spoofing vulnerability in the RADIUS protocol of Juniper Networks Junos OS and Junos OS Evolved platforms allows an on-path attacker between a RADIUS server and a RADIUS client to bypass authentication when RADIUS authentication is in use. Please refer to https://supportportal.juniper.net/JSA88210 for more information.PR1850776

Services Applications

- On SRX5K HA cluster in FIPS mode, repeated manual failovers of redundancy groups can result in SPC3 or IOC4 or both the cards going offline.PR1797468

Unified Threat Management (UTM)

- Avira is not supported for SRX4700 in 24.4R1-S2PR1851627

Resolved Issues

IN THIS SECTION

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

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 SRX platform may experience a flowd process crash and generate core dump files when the ALG feature is enabled PR1852968

Chassis Clustering

- FIPSCC - SRX5k L2HA (link-encryption) - Traffic through customer ipsec vpn tunnel halts/stops after back to back failover until rekey occurs PR1842874
- L3MNHA with SRG1 IPSEC : MNHA ICL ipsec encryption link went down permanently after rebooting connected router through which ICL was established before. During this state IKE process got stuck at ~70% on MNHA Active node. PR1850967
- Post chassis-control restart on one of MNHA node, Node goes into OFFLINE [SP] status with SRG in INELIGIBLE state and does not recover from this state PR1873432

Flow-based and Packet-Based Processing

- AppQoS rate limit in PMI mode on SRX5K and SRX4600 may drop packets unexpectedly PR1828819
- [False Drop messages for defrag traffic] Packet-drop records with fragmented traffic ",Dropped by FLOW:Defrag return error" seen on " show security packet-drop records " PR1833132
- GRE traffic is getting blocked due to a software programming issue and MTU going below minimum value PR1834338
- Type 5 VXLAN traffic drops are observed when SRX run as L3-VNI gateway and the ingress and egress traffic goes to the same Type-5 VXLAN peer PR1847419
- Junos SRX platforms with chassis cluster configured experience flowd crash due to a race condition in multicast session handling PR1854492
- Data Plane CPU on one device spikes up to 95% during primary node system reboot in SRX cluster PR1856521
- The flowd process crash when service offload and system stats are enabled PR1859062
- SRX4700 custom application session inactive timeout is half of the configured value PR1865294

- PFE crash is observed when PFE processes the traffic passing through the dedicated fabric link PR1872613
- The TCP session is not closing properly on the SRX4600 and SRX5K platforms after receiving the FIN-ACK message causing packets to drop for new session if reusing same source port PR1873580
- SRX platforms drops MPLS traffic when "gre-performance-acceleration" knob is enabled PR1876356

General Routing

- Multiple J-UKERN core files might be generated during the sanity test PR1641517
- ifHCOutOctets unexpected spikes in value PR1706125
- Crash dump on DNSF plugin observed on SRX platforms PR1816951
- RTO traffic loss and accumulation of session on secondary node is observed when RTO traffic not evenly distributed to all FLT (Flow Thread) threads PR1819911
- On SRX4600 platforms with heavy traffic, the FPGA drops packets PR1823577
- The rpd crash is observed during upgrade or restart PR1826194
- On SRX platforms MLD groups are successfully formed however egress traffic is not being forwarded as expected PR1828211
- The SRX1500 drops the packet if MTU matches the MRU of the receiving device PR1831955
- The IDP security-package install is throwing 'Attack DB Update Failed' error and AppID stops working PR1832094
- Custom application detection fails for L4 traffic after upgrade due to uncompiled signatures PR1833667
- AE interfaces not coming up if configured with flexible-vlan-tagging and output-vlan-map. PR1838033
- Traffic loss due to tunnel establishment failure in HA setup PR1839090
- Load balance hash-key forwarding persists when switching to Layer 3-only PR1842873
- Split brain condition will be seen in SRX4600 configured in Chassis Cluster under certain conditions PR1843413
- Application crash is observed due to insufficient memory when a large number of JFlow entries are created PR1843679

- Unnecessary trace log files related to licenses are generated PR1845079
- SRX PFE crash is observed with source-identity enabled PR1845506
- Auto-re-enrollment for local certificate once fail, not trigger again on SRX platforms PR1845573
- Security-metadata streaming is impacted due to dynamic-filter issue PR1845645
- Packet drops are observed in the VPLS environment on SRX380 platforms in packet mode PR1845997
- FPC0 will not transition to Online and may generate chassis alarm "FPC 0 Hard errors" in SRX4600 devices deployed in chassis cluster PR1846340
- Core being generated for some processes while using license feature PR1848160
- Local or peer device's interface reflects down after SRX380's reboot PR1848557
- It is not recommended to restart chassisd using CLI command "restart chassis-control" in MNHA setup PR1849108
- Reth Reserved buffer increases when reth interface is activated PR1849364
- The commit command failed due to a speed mismatch between the Ten-Gigabit Ethernet (XE) port and the Aggregated Ethernet (AE) interface to which it belongs PR1851261
- Traffic reduction observed for SWP sessions when traffic hits SWP as passthrough. PR1851686
- Flexible-vlan-tagging option is missing under interface hierarchy on SRX3xx series PR1853238
- PIM IP ESP packet fragments dropped in SRX platform PR1854130
- The nsd process crashes on SRX platforms during cluster reboot, failover, or policy addition causes traffic outage PR1857379
- The chassisd process crash is seen after the device reboot when chassisd stalls after configuration commit PR1857833
- Security log report messages w.r.t logical system is not generated PR1860597
- Packet drops can occur when packets are received with a size equal to the default MRU PR1863576
- CoS shaping is not functional on IRB interfaces when the SRX1600 is in switching mode PR1868103
- TCP RST packet gets dropped when used with rst-invalidate-session PR1873583
- Commit Delay Due to Incomplete MACsec Pre-Shared Key Configuration PR1873885
- Unexpected primary role assignment on SRX after node0 reboot PR1877323

- ISSU getting aborted due to configuration-synchronize failure on Junos SRX platforms PR1882569

J-Web

- Created address-sets in global address book is not visible in J-Web PR1805828
- [SRX Jweb] Junos image upload progress message is not displayed on Branch SRX platform PR1844395
- [Jweb] Gratuitous ARP Count shows 0 for redundancy group 1+ when the default gratuitous-arp-count value is used PR1845747
- Unable to load J-Web after upgrading SRX when time zone is set to GMT+x or GMT-x. PR1851362
- VPN failures on SRX due to file descriptor issue PR1858466

Network Management and Monitoring

- SNMPV3 Engine-ID does not update to MAC address as configured PR1866948

Platform and Infrastructure

- The self-generated traffic on Junos platforms use the incorrect source IP with ECMP configuration PR1849296

Routing Policy and Firewall Filters

- The "show security match-policies" command results in a timeout error PR1809563
- [SRX] - RE and PFE policy out of sync with specific configuration. PR1837182
- Security flow sessions are impacted during ISSU on SRX platforms PR1838698
- The mgd process crash is observed during large amount of configurations PR1847877
- Wrong service-name display in SRX RT_FLOW traffic log. PR1859554

- Deny traffic log message is not generated for persistent nat traffic PR1869988
- Protocols involved with TCP/IP on a lsi interface have issues as TCP 3-way handshake cannot be completed PR1871431

Routing Protocols

- The rpd crash on commit when configuring router-advertisement with DNS search label under 3 characters PR1847811
- Updating a source-file to load ROAs should be done by changing the name of the source file PR1853025

Unified Threat Management (UTM)

- The utmd process crashes when EWF or NG web-filtering is configured on SRX with scaled custom URLs PR1841370
- FPC crashing when web filtering type set to "juniper-enhanced" or "NG-juniper" PR1854519

User Interface and Configuration

- XML namespace string in rpc-reply tag for system-uptime-information was changed to represent the full version name. PR1842868

VLAN Infrastructure

- On SRX platforms, STP multicast packets are discarded, causing PVST to fail to converge between switches PR1831324
- Traffic drops are observed when SRX380 platform is configured in l2 transparent-bridge mode PR1852047
- PFE crash due to invalid cached next hop during reinjection on SRX5k PR1856200

VPNs

- Master-encryption-password is not accessible when system is in FIPS mode PR1665506
- The flowd process crashes on SRX5K platforms with multiple line cards in MNHA scenario PR1839665
- ICL link encryption should be used for connection between pub-broker sub-broker with loopback interface IP's should be used with to avoid IPsec session sync failure between master and backup MNHA devices. PR1840788
- L3MNHA with SRG1 IPSEC : "show chassis high-availability information" cli says SRG1 control plane state as Ready eventhough ICL connection between Pub-Broker Sub-broker is not established properly and IPsec sessions are not syncing between Master and Standby MNHA peers. PR1840803
- FIPS-CC:SRX-SME(Berkeley-FreeBSD12): IPSEC sa_config entries on node0 PFE are empty when configured from secondary node. PR1846168
- IKED core might be observed during a restart or failover event. PR1848834
- SRX fails to renegotiate VPN with the correct gateway when the active tunnel goes down PR1851652
- Recommended command to failover from Primary to Backup node PR1861056
- On rare circumstances the kmd or iked process crash will be observed on using the third-party library API PR1864322
- Post reboot , IPSec VPN is not coming up over MNHA active/active deployment PR1864758
- Tunnel sync failure on backup node post 'restart chassis-control' in MNHA Active-Active mode PR1866890
- Type 5 EVPN traffic is dropped on SRX when PMI is disabled or not supported PR1867040
- IPSec tunnel inactive after multiple srg failovers on SRX platforms PR1868453

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

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

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

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

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

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

Table 7: EOL and EEOL Releases

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

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

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

Documentation Updates

This section lists the errata and changes in Junos OS Release 24.2R2 for the SRX Series documentation.

Junos OS Release Notes for vSRX

IN THIS SECTION

What's New

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

What's Changed

IN THIS SECTION

Learn about what changed in this release for vSRX.

User Interface and Configuration

- **The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX and vSRX)**—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

- **Access privileges for request support information command (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance` , `view` , and `view-configuration` can execute request support information command.

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the `Hostname` field first instead of last. The `show version` command output includes the `Family` field. The `Family` field identifies the device family under which the device is categorized, for example, `junos`, `junos-es`, `junos-ex`, or `junos-qfx`.

  [See show system information and show version.]

VPNs

- **Enhancements to fix the digest option functionality for key pair generated with DSA and ECDSA (SRX Series and vSRX 3.0)**–In earlier releases, when you generated local self-signed certificates using sha-256 digest and DSA or ECDSA encryption using `request security pki generate-key-pair certificate-id` *`certificate-id-name`* `size` *`size`* `type (dsa | ecdsa)` and `request security pki local-certificate generate-self-signed certificate-id` *`certificate-id-name`* `digest sha-256 domain-name` *`domain-name`* `subject` *`subject-distinguished-name`* commands, the generated signature always used sha1 digest. Starting this release, the specified digest, sha-256, is used for the signature digest. You can verify using `show security pki local-certificate certificate-id` *`certificate-id-name`* `detail`

- **Enhancement to the output of clear and regenerate key pair commands (vSRX 3.0)**–We've modified the output of the following commands when you clear and regenerate the same key pair to manage the secure data using hardware security module (HSM).

  Starting in Junos OS 23.4R1 release, the command:

  - `clear security pki key-pair certificate-id` *`certificate-id-name`* displays the message `Key pair deleted successfully from the device. Key pair will be purged from the keyvault based on it's own preferences`, as opposed to the message `Key pair deleted successfully` displayed in previous releases.

  - `request security pki generate-key-pair certificate-id certificate-id-name` displays the message `error:Failed to generate key pair. If the keypair was created and deleted before, please ensure that the keypair has been purged from the keyvault` as opposed to the message `error: Failed to generate key pair` displayed in previous releases.

  We made these changes to align with the cloud provider's restriction on key pair deletion, if any.

- **Enhancements to the help string description for the threshold and interval options for VPN monitoring options (SRX Series and vSRX 3.0)**–We've enhanced the help string description of the `threshold` and `interval` options available in the configuration statement `[set security ipsec vpn-monitor-options]` to include the default values. You'll see the following description with the default values:

  ```
  user@host# set security ipsec vpn-monitor-options ?
  Possible completions:
  interval Monitor interval in seconds Default :10 (2..3600 seconds)
  threshold Number of consecutive failures to determine connectivity Default :10 (1..65535)
  ```

  [See ipsec (Security).]

- **Enhancements to the output of show security ipsec security-associations detail command (SRX Series and vSRX 3.0)**–We've enhanced the output of `show security ipsec security-associations detail` when you enable `vpn-monitor` at the `[edit security ipsec vpn` *`vpn-name`*`]` hierarchy level, when your firewall

runs IPsec VPN services with the new iked process. The output displays `threshold` and `interval` values in the command output. Starting in Junos OS Release 23.4R1, you'll notice these changes.

[See show security ipsec security-associations.]

- **Reauthentication frequency recommendation for IPsec VPN with PPK (SRX Series and vSRX 3.0)**—For IPsec VPN, including the Auto Discovery VPN (ADVPN), with post-quantum pre-shared key (PPK) encryption, when the IKE security association is negotiated with the quantum keys, the iked process performs rekeying after 4 seconds to secure the channel. If you set the reauthentication frequency to 1, rekeying doesn't happen after 4 seconds. So we recommend you to set the reauthentication frequency to more than 1 as the first reauthentication count is used by the PPK default rekey.

  [See Quantum Safe IPsec VPN.]

Known Limitations

IN THIS SECTION

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.

Platform and Infrastructure

- In the case of MNHA GCP deployment, if a name-server should be configured, then it should be configured along with google's metadata DNS server (169.254.169.254)PR1829939

Open Issues

IN THIS SECTION

Learn about open issues in this release for vSRX.

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

General Routing

- On Junos SRX5600 and vSRX3 platforms while upgrading from an older JUNOS version to 22.4R3-S1 or 22.4R3-S2, the upgrade process can fail as the rpd crashes as part of validation process. This is seen if the router config has Multicast/Internet Group Management Protocol (IGMP) or Broadband Edge configuration.PR1810817
- Found that for this tenant_id : s3idh8g4cbe4p5pk we had 64 feeds in SecProfiling category, but only 19 feeds are stored in CDB - secintel_feeds. Because of this only 19 feeds were listed on UI. But while creating a new feed, it is checking if new SecProfiling feeds can be created for the tenant_id in schedule DDB table . Since we have already 64 (which is the max number of feed per tenant)feeds in DDB table, it throws an error - Feed creation error: Feed count limit(64) reached for category: SecProfiling. After running the scripts to create feeds, we need to have scripts to delete the feeds from DDB too so that the data will be accurate during testing. I have removed unwanted entries from DDB table(Now only 20 feeds for the tenant). From now new feeds can be created for Adaptive Threat Profiling sectionPR1819444
- As per OpenSSH 9.0/9.0p1 release notes: "This release switches scp(1) from using the legacy scp/rcp protocol to using the SFTP protocol by default." In this case, since we are running OpenSSH 9.0 and above- OpenSSH_9.7p1 , this uses the "SFTP" protocol by default when scp command is invoked from shell. However, vSRX3.0 supports the "SCP" protocol by default when scp command is invoked. So to use the legacy "SCP" protocol from shell, please use the -O command line option For example: scp -O other options/arguments Note: Incoming SCP connections from outside hosts that are running OpenSSH version 9.0/9.0p1 could fail since sftp-server is disabled by default in Junos OS . Hence, users should either use the -O option on remote host while initiating scp file transfer OR

enable sftp-server in the Juniper configuration. To enable sftp-server in Juniper configuration, use the following hierarchy: "set system services ssh sftp-server"PR1827152

- On SRX3xx series configured with native-vlan-id, after upgrading an SRX3xx series device to Junos version 23.4R1 or higher, the native-vlan-id option disappears from the interface settings. If native-vlan-id was set before the upgrade, the device keeps the setting but it doesnt apply it to the interface. Trying to delete native-vlan-id causes a syntax error. The native-vlan-id feature doesn't work, and if a custom VLAN ID (other than 1) was used then traffic for that VLAN will be affected.PR1847366

Network Address Translation (NAT)

- The existing RSI misses out on few important information from NAT plugin, which can now be collected via a new RSI CLI command - "request support information security-components nat". This will provide more data and help in better debugging.PR1825372

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for vSRX.

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

Flow-based and Packet-Based Processing

- In vSRX orphan backup sessions will exhaust session resources due to high backup session timeout value PR1846897
- Type 5 VXLAN traffic drops are observed when SRX run as L3-VNI gateway and the ingress and egress traffic goes to the same Type-5 VXLAN peer PR1847419
- Data Plane CPU on one device spikes up to 95% during primary node system reboot in SRX cluster PR1856521
- SRX platforms drops MPLS traffic when "gre-performance-acceleration" knob is enabled PR1876356

General Routing

- Crash dump on DNSF plugin observed on SRX platforms PR1816951
- RTO traffic loss and accumulation of session on secondary node is observed when RTO traffic not evenly distributed to all FLT (Flow Thread) threads PR1819911
- IKE SAs tunnel is down for IPv6 with IKEv1 on NFX350 PR1832087
- Dedicated-offload-cpu requires a full restart of vSRX 3.0 in 24.4R1 PR1842550
- Auto-re-enrollment for local certificate once fail, not trigger again on SRX platforms PR1845573
- vSRX3.0 kernel panic when deployed in Qemu version 8.1 and above PR1845886
- PIM IP ESP packet fragments dropped in SRX platform PR1854130
- Split brain scenario is observed on vSRX3.0 with public cloud MNHA deployment PR1855010
- Cloud Instances (GCP/Azure/AWS): Missing vCPU After Downgrading from Image 25.2 to Lower Versions PR1871397
- The srxpfe process crash is observed on vSRX platform after set disable on the ge- interface and then rollback PR1874848
- On vSRX3.0 platforms, MNHA link fails to come up when MNHA ICL tunnel is enabled alongside dedicated-offload-cpu PR1875491
- [SRX_TYPE_5_USECASE] When source and dest VRF is present in match criteria of a security policy, policy match does not work for vxlan traffic PR1884150

Platform and Infrastructure

- FTP default mode changed from active to passive on 24.2R2 PR1874525

Routing Policy and Firewall Filters

- Failed inter-process communication results in higher heap and buffer usage which impacts the functionality of processes PR1823591

Routing Protocols

- Updating a source-file to load ROAs should be done by changing the name of the source file PR1853025

VPNs

- ICL link encryption should be used for connection between pub-broker sub-broker with loopback interface IP's should be used with to avoid IPsec session sync failure between master and backup MNHA devices. PR1840788
- L3MNHA with SRG1 IPSEC : "show chassis high-availability information" cli says SRG1 control plane state as Ready eventhough ICL connection between Pub-Broker Sub-broker is not established properly and IPsec sessions are not syncing between Master and Standby MNHA peers. PR1840803
- IPSEC tunnel distribution table on the RE is not cleaned up hitting SRXPFE coredump eventhough DPD is configured. PR1850526
- On vSRX 3.0 platform IPSec tunnels do not redistributed with dedicated-offload-cpu knob enabled PR1860693

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 24.2R1 for vSRX using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

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

The following limitations apply:

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

  Check this using the following command:

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

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

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

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 24.2R1 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
       24.2K 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 24.2R1 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-x86-64-24.2-2024-06-06.0_RELEASE_24.2_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-
x86-64-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 24.2 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-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-24.2-2024-06-06.0_RELEASE_24.2_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-24.2-2024-06-06.0_RELEASE_24.2_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-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-24.2-2024-06-06.0_RELEASE_24.2_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-24.2-2024-06-06.0_RELEASE_24.2_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-24.2-2024-06-06.0_RELEASE_24.2_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 24.2R1 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 24.2-2024-06-06.0_RELEASE_24.2_THROTTLE Kernel 64-bit
JNPR-11.0-20240606.170745_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: 24.2-2024-06-06.0_RELEASE_24.2_THROTTLE
JUNOS OS Kernel 64-bit  [20240606.170745_fbsd-builder_stable_11]
JUNOS OS libs [20240606.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20240606.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20240606.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20240606.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20240606.170745_fbsd-builder_stable_11]
JUNOS py extensions [20240606.110007_ssd-builder_release_174_throttle]
JUNOS py base [20240606.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20240606.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20240606.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20240606.110007_ssd-builder_release_174_throttle]
JUNOS libs [20240606.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20240606.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20240606.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20240606.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20240606.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20240606.110007_ssd-builder_release_174_throttle]
JUNOS modules [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20240606.110007_ssd-builder_release_174_throttle]
```

```
JUNOS srxtvp libs [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20240606.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20240606.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20240606.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20240606.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20240606.110007_ssd-builder_release_174_throttle]
```

Validating the OVA Image

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

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

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

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

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

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

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

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

Table 8: EOL and EEOL Releases

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

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

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

Licensing

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

The major components of the framework are:

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

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

Finding More Information

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

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

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

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

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

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

  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/

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.

- 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

4 December 2025—Revision 9, Junos OS Release 24.2R2.

11 November 2025—Revision 8, Junos OS Release 24.2R2.

03 October 2025—Revision 7, Junos OS Release 24.2R2.

07 August 2025—Revision 6, Junos OS Release 24.2R2.

10 July 2025—Revision 5, Junos OS Release 24.2R2.

30 May 2025—Revision 4, Junos OS Release 24.2R2.

15 May 2025—Revision 3, Junos OS Release 24.2R2.

31 March 2025—Revision 2, Junos OS Release 24.2R2.

28 February 2025—Revision 1, Junos OS Release 24.2R2.