Release Notes

Published
2025-01-17

Junos OS Release 22.3R1®

Juniper Networks | Engineering Simplicity

Table of Contents

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion Enterprise, Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX. These release notes accompany Junos OS Release 22.3R1. 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.

Key Features in Junos OS Release 22.3

Start here to learn about the key features in Junos OS Release 22.3. For more information about a feature, click the link in the feature description.

- **Access Gateway Function (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 22.3R1, we introduce the Access Gateway Function (AGF). AGF provides wireline traffic convergence by interworking wireline connected devices with the 5G Core (5GC). AGF is the access point for existing fixed network residential gateway (FN-RG) and is an integral part of the Junos Multi-Access User Plane solution. AGF supports the following capabilities:
  - DHCP relay and DHCPv6 stateful relay service for relay client negotiations to a DHCP server in the 5GC
  - PPPoE access to the 5GC
  - N1 proxy signaling for user equipment (UE) registration and Protocol Data Unit (PDU) session establishment procedures for FN-RG authentication, address assignment, and authorization
  - N2 signaling with the Access and Mobility Management Function (AMF)
  - N3 signaling to both an external and colocated user plane function (UPF) that supports per subscriber IP and IPv6 data connectivity to a data network
  - UE-level QoS that originate from the 5GC authorization
  - Colocation of AGF, broadband network gateway (BNG), and UPF services on a single MX Series router

  You can configure AGF services in the `[edit services agf]` hierarchy.

[See AGF User Guide.]

- **SCTP support (MX204, MX240, MX480, MX960, and MX10003)**—In Junos OS Release 22.3R1, you can configure SCTP to connect the Access Gateway Function (AGF) with the Access and Mobility Management functions (AMFs). SCTP is a reliable connection-oriented protocol that you use for transporting message streams.

  - Multistream protocol
  - User data fragmentation
  - Chunk bundling
  - Packet validation
  - Multihome support

  AGF creates an SCTP association to communicate with the AMFs. You can configure the SCTP association in the `[edit services agf amf]` hierarchy.

  Use the `show system connections | find sctp` command to check the SCTP endpoints and associations.

  Use the `show system statistics sctp` command to query the SCTP system-wide statistics.

  [See AGF User Guide, show system statistics, and show system connections.]

- **Support for Multi-Access User Plane (MX10004)**—Starting in Junos OS Release 22.3R1, LC2101 and LC480 line cards support Junos Multi-Access User Plane functions.

  [See Multi-Access User Plane User Guide.]

Junos OS Release Notes for ACX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

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

Junos Telemetry Interface

- **BGP policy sensor upgrade (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10002, and vRR)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports data model **openconfig-bgp-policy.yang** version 6.0.2 (upgraded from version 4.0.1). JTI also supports new BGP policy sensors.

  [See Telemetry Sensor Explorer.]

- **Support for MPLS RSVP-TE sensors (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, and PTX10002)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports data model **openconfig-mpls-rsvp.yang** version 4.0.0. It supports new RSVP-TE sensors.

  [See Telemetry Sensor Explorer.]

- **Support for MPLS OpenConfig configuration and sensors (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, and PTX10002)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports the following data models:

  - **openconfig-mpls.yang** version 3.2.2
  - **openconfig-mpls-types.yang** version 3.2.1
  - **openconfig-mpls-te.yang** version 3.2.2
  - **openconfig-mpls-static.yang** version 3.2.2

  JTI supports the following OpenConfig configurations:

  - MPLS global
  - MPLS `named-explicit-path`
  - MPLS tunnels

  JTI supports the following state groups:

  - MPLS tunnels
  - MPLS `named-explicit-path`
  - MPLS static `label-switched-path`
  - MPLS-TE interface attributes
  - MPLS tunnel state counters (dependent on the Packet Forwarding Engine)

  [See Telemetry Sensor Explorer and Mapping OpenConfig MPLS Commands to Junos Configuration.]

- **Support for VLAN sensors (ACX5448, ACX5448-M, ACX5448-D, and ACX710 routers, EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC and EX9208 switches, MX204, MX240, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2010, MX2020, PTX10008, and PTX10016 routers and vMX)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports the data model **openconfig-vlan.yang** version 3.2.1, including sensor support to stream VLAN and MAC- limit operational states through telemetry.

  [See Telemetry Sensor Explorer.]

OpenConfig

- **Support for OpenConfig VLAN model (ACX5448, MX10003, PTX10008, QFX5110, and QFX10002)**—Starting in Junos OS Release 22.3R1, we support the OpenConfig VLAN data model **openconfig-vlan.yang**, version 3.2.1. You can use paths for configuration and for streaming of operational state data.

  [For operational state paths, see Telemetry Sensor Explorer. For configuration, see Mapping OpenConfig VLAN Commands to Junos Configuration.]

- **Support for OpenConfig BFD configuration and state (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, and PTX10002)**—Starting in Junos OS Release 22.3R1, we support OpenConfig configuration and state support for BFD. Use BFD telemetry data to detect failures in the forwarding path between two adjacent routers.

  [See Mapping OpenConfig Interface Commands to Junos Configuration and Telemetry Sensor Explorer.]

- **OpenConfig IS-IS configuration support (ACX5448, ACX710, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX3000, PTX10002, and PTX10003)**—Starting in Junos OS Release 22.3R1, we support IS-IS configuration using OpenConfig.

  [See Mapping OpenConfig ISIS Commands to Junos Configuration.]

Routing Protocols

- **Strip and replace BGP private-AS path (ACX710, JRR200, MX480, PTX10001, QFX5220, and QFX10003)**—In Junos OS Release 22.3R1, we have introduced the `strip-as-path` policy option that removes the incoming autonomous system (AS) path as part of the import policy for a BGP session and replaces the received autonomous system (AS) path with the receiving router's local AS number for the receiving session. Note that the local AS number may be different from the number configured under `autonomous system` in the `[edit routing-options]` hierarchy.

  If you need to normalize externally injected routes, you can use this policy option for the incoming autonomous system (AS) path so that it may be used similarly to routes that originate solely within the fabric. The new `strip-as-path` policy option has no impact on the BGP export policy.

  You can configure the `strip-as-path` option under `policy-options then` clause:

  ```
  set policy-options policy-statement do-strip term a then strip-as-path
  ```

  [See Autonomous Systems for BGP Sessions.]

Additional Features

We've extended support for the following features to these platforms.

- **Real-time performance monitoring (RPM) IPv4/IPv6 client with Routing Engine and Packet Forwarding Engine timestamping, RPM IPv4/IPv6 server with Packet Forwarding Engine timestamping, Two-Way Active Measurement Protocol (TWAMP) managed IPv4 client and server, TWAMP Light IPv4/IPv6 client and server** (ACX710 and ACX5448)

  [See Understanding Using Probes for Real-Time Performance Monitoring and Understand Two-Way Active Measurement Protocol.]

- **RPM-tracked static routes** (ACX710 and ACX5448)

  [See rpm-tracking and show route rpm-tracking.]

- **Supported transceivers, optical interfaces, and direct attach copper (DAC) cables**. Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update this tool and provide the first supported release information when the optic becomes available.

What's Changed

There are no changes in behavior and syntax in this release for ACX Series routers.

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.

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 `no-validate` statement. PR1568757

Open Issues

IN THIS SECTION

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

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

General Routing

- VXLAN VNI (multicast learning) scaling on traffic issue is seen from VXLAN tunnel to L2 interface. PR1462548
- Due to BRCM KBP issue route lookup might fail. Need to upgrade KBP to address this issue. PR1533513
- Service MIC does not work on ACX500 running Junos 20.4 or higher. PR1569103
- The issue occurs on ACX5448, MX204, and MX2008 "VM Host-based" platforms. Starting with Junos OS Release 21.4R1 or later, use ssh and root login to copy line card image (chspmb.elf for MX2008) from Junos VM to Linux host during installation. Installation requires ssh and root login. Use `deny-password` instead of `deny` as default root-login option under ssh configuration to allow internal trusted communication. See TSB18224. PR1629943
- On Junos ACX platforms (ACX1100, ACX2100 and ACX2200) the FEB crash might occur. This crash might occur only when the system has encountered a dual parity error on MPLS entry memory in the hardware. There might be an impact on services when the FEB crashes, however, it returns to normal functionality after the crash. PR1632043

- Interop for 1G interfaces between EX4100 SKUs and ACX5448/ACX5448-M/D or MX480 might not work. PR1657766
- It is a negative use case and happens when you commit an incorrect configuration and boot the box. PR1658327
- For MX204, MX10003, and ACX5448 platforms, if you configure a non-default ssh port for system login, after upgrade to Junos OS Release 21.4, the FPC might get stuck in offline. To avoid such issue, use default SSH port and use protect Routing Engine filter to only allow the access from the trusted source.PR1660446
- In VPLS MH cases, the standby UNI logical interface in backup router is programmed in disable state, by adding the UNI interface to invalid vpn id in HW. During switchover, the UNI logical interface will be deleted and added under the VPLS instance VPN id. In issue case, UNI interface added under invalid VPN id in backup router tries to be deleted by passing the VPLS instance vpn id, causing the issue. This issue is applicable only for ACX5000 Series routers. PR1665178
- When you connect more than 1 DHCP server to the device and initiate zeroize, it adds multiple routes and the fileserver becomes unreachable after the zeroize if it is not reachable through the default route.PR1675011

Resolved Issues

IN THIS SECTION

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

General Routing

- On Junos platforms, if you change CCM configuration from aggregated Ethernet logical interface to the physical logical interface in a single commit, you might see cfmd core files in the logs. PR1612212
- Tx stuck issue might trigger a major alarm DPDK. PR1626562
- VLAN priority might change at the egress end of the circuit. PR1630255

- Late drops are not at par with PN configured. PR1630724
- The ARP request packets might be sent out from ACX router without VLAN header. PR1638421
- A missing component in the dump kernel might prevent the ACX-710 router from rebooting after generating the file. PR1639459
- KRT queue entries get stuck during Routing Engine switchover when backup RPD is not yet ready. PR1641297
- The mcsnoopd crash occurs while adding igmp-snooping. PR1641497
- Attributes are showing as "Unknown_Attribute" while verifying smartd parameters in ACX5448-M. PR1643542
- In EVPN multihoming, BUM traffic from the CE device floods back to the CE device. PR1643598
- Reboot reason is not as expected for ACX5448-M. PR1643781
- The copper ports on ACX5448 might go down if loaded with copper SFP. PR1643989
- Traffic drop might be seen on the interfaces that use copper SFP after the reboot. PR1645396
- The swap-push/pop-swap VLAN map operations on VPLS logical interface might not work. PR1648182
- While sending BGP NOTIFICATION messages for RFC 8538 HARD RESET, the data portion is sometimes not present. PR1648479
- If a firewall has a log action and you applied on physical interface or lo0, the LDP cannot go up. PR1648968
- BGP Sensor `/bgp-rib/afi-safis/afi-safi/ipv4-unicast/loc-rib/`is not available as a 'periodic' sensor. PR1649529
- On all Junos ACX platforms, priority tagged packets drop due to an untagged Aggregated Ethernet interface. PR1650970
- PCS faulty blocks count will increment after Junos software upgrade to Junos OS Release 20.2R1 or above. PR1651526
- HTTP(S) file download hangs over EVPN-ETREE. PR1653531
- Due to the MAC learning limit being exceeded, you might observe traffic drop in the MC-aggregated Ethernet scenario. PR1653926
- The LDP sessions might flap in VPLS scenario resulting in Packet Forwarding Engine errors. PR1654172

- The validation fails if you perform a media install Junos upgrade. PR1657840
- On ACX5448 platform, physical interfaces of FPC remain up even though it lost communication with Routing Engine. PR1659949
- Packet count shown as 0 for some interfaces in `monitor interface traffic`. PR1661617
- The l2circuit backup might not get reverted to primary in rare condition. PR1661802
- Transit traffic drop was seen for Border Gateway Protocol-Labeled Unicast (BGP-LU) prefix on ACX5448/ACX710 when BGP-LU label routes have ECMP forwarding path. PR1663563
- In the SR-TE scenario, sensors populate incorrectly for colored tunnel BSID routes when you enable uncolored tunnels. PR1665943
- On ACX710 and ACX5448, its variants Packet Forwarding Engine might crash due to configuration of BFD. PR1667129
- Shutting the CE interface and bringing back up causes traffic (going toward the core file) drop. PR1667724
- LLDP neighborship might fail if the chassis-id format of the LLDP packet is xx:xx:xx:88:8e:xx. PR1669677
- Chassis alarms for smart errors are not set or cleared. PR1669968
- ACX710: Log related to resources reported after EVPN RI are deactivated / activated multiple times: `ACX_BD_ERR: dnx_bd_alloc_l2_svlan: System reached L3 IFL and BD limit(12286)`. PR1670683
- The chassisd memory got corrupted and then crashed. PR1672039

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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

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

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

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

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 1: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Junos OS Release Notes for cRPD

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for the containerized routing protocol process (cRPD) container. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

Learn about new features introduced in the Junos OS main and maintenance releases for cRPD.

Additional Features

We've extended support for the following features to these platforms.

- **Support for virtual router redundancy protocol (VRRP)** (cRPD)

  [See cRPD with VRRP.]

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R1 for cRPD.

Known Limitations

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

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 cRPD.

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 which issues were resolved in the Junos OS main and maintenance releases for cRPD.

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

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for cRPD.

Platform and Infrastructure

- Kernel logs on cRPD containers running on the same host are incomplete. PR1668794
- Block all the unsupported CLI configuration statements and operational commands on cRPD. PR1673671
- The show interfaces intf-name command lists all the interfaces. PR1674333

Junos OS Release Notes for cSRX

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for the cSRX Container Firewall, a containerized version of the SRX Series Services Gateway. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R1 for cSRX.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R1 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

IN THIS SECTION

Resolved Issues

There are no resolved issues in this release for cSRX.

Junos OS Release Notes for EX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for EX Series Switches.

Hardware

- **New EX4100 Multigigabit switches and EX4100-F switches**—Starting in Junos OS Release 22.3R1, we introduce the EX4100 multigigabit family of switches and the compact fanless switches (EX4100-F-12P and EX4100-F-12T) that provide connectivity for high-density environments and scalability for network growth. You can deploy the EX4100 multigigabit switches in modern campus and branch enterprise networks. We support 24-port and 48-port switch variants with POE++ RJ-45 ports. The switches have dedicated Virtual Chassis ports (VCPs) and uplink ports.

  We support the following switches: EX4100-48MP, EX4100-24MP, EX4100-F-12P, and EX4100-F-12T.

Table 2: Features Supported on EX4100-48MP, EX4100-24MP, EX4100-F-12-P, and EX4100-F-12-T

Feature	Description
Chasssis	• Support for FRU management, environment monitoring, and chassis support, including: • PSU, fan, and temperature sensors monitoring • (EX4100-48MP, EX4100-24MP only) Power management support for two power supply units (PSUs) and two field-replaceable fans. The system functions with one fan until it reaches shutdown temperature. • When temperature reported by various sensors crosses the specified threshold, the fan speed increases or decreases to regulate the temperature. If the temperature exceeds the shutdown threshold, system shutdown is initiated. • Watch timer update during bootup. The CPU default watch time-out is 35 sec. [See Understanding Power Management on EX Series Switches.]

Table 2: Features Supported on EX4100-48MP, EX4100-24MP, EX4100-F-12-P, and EX4100-F-12-T *(Continued)*

Feature	Description
Hardware	• New EX4100 switch models – We've introduced the following EX4100 ethernet switch models - EX4100-24MP, EX4100-48MP, EX4100-F-12T, and EX4100-F-12P. The following are the salient points of the switch models. • EX4100-24MP – Eight 1/2.5/5/10-Gbps and sixteen 1-Gbps PoE++ RJ-45 ports; four 10/25-Gbps SFP28 Virtual Chassis ports and four 1/10-Gbps SFP+ uplink ports – all these ports are located on the front panel. EX4100-24MP is powered by AC power supplies and has AFO cooling. • EX4100-48MP - Sixteen 1/2.5-Gbps and thirty-two 1-Gbps PoE++ RJ-45 ports; four 10/25-Gbps SFP28 Virtual Chassis ports and four 1/10-Gbps SFP+ uplink ports – all these ports are located on the front panel. EX4100-48MP is powered by AC power supplies and has AFO cooling. • EX4100-F-12P – Twelve 1-Gbps PoE+ RJ-45 ports, four 10-Gbps SFP+ Virtual Chassis ports – all of these ports are located on the front panel. Two 1/2.5/ 5/10-Gbps Base-T multigigabit Ethernet PoE-powered uplink ports – are located in the back. The EX4100-F-12P can be powered by AC power or as a powered device. The device has natural convection cooling. • EX4100-F-12T – Twelve 1-Gbps non-PoE RJ-45 ports, four 10-Gbps SFP+ Virtual Chassis ports – all of these ports are located on the front panel. Two 1/2.5/ 5/10-Gbps

Table 2: Features Supported on EX4100-48MP, EX4100-24MP, EX4100-F-12-P, and EX4100-F-12-T *(Continued)*

Feature	Description
	Base-T multigigabit Ethernet uplink ports – are located in the back. The EX4100-F-12T is powered by AC power. The device has natural convection cooling. [See EX4100 Hardware Guide]. • The EX4100-F-12P switch will support powered device functionality. In addition to being powered by AC power, the EX4100-F-12P switch can be powered by another PoE-enabled EX4100 switch. [See EX4100 Hardware Guide].
High Availability and resiliency	• Resiliency support for inter-integrated controller (I2C), disk failure, and disk health. [See High Availability User Guide.]

Table 2: Features Supported on EX4100-48MP, EX4100-24MP, EX4100-F-12-P, and EX4100-F-12-T *(Continued)*

Feature	Description
Interfaces	• EX4100-48MP, EX4100-24MP, EX4100-F-12P, and EX4100-F-12T support the following speeds: • EX4100-48MP • Downlink ports on PIC 0 (ports 0 - 47). The first 16 are multi-rate ports that support 100-Mbps, 1-Gbps, and 2.5-Gbps. The remaining 32 ports are GigE ports that support 10-Mbps, 100-Mbps, and 1Gbps. • VCPs (ports 0–3 on PIC 1) support 4x1-Gbps or 4x10-Gbps or 4x25-Gbps speeds. If you convert the VCPs to network ports, ports 0 through 3 on PIC1 support 1-Gbps or 10-Gbps or 25-Gbps speeds • Uplink ports (ports 0–3 on PIC 2) support 4x10-Gbps or 4x1-Gbps speeds. • EX4100-24MP • Downlink ports on PIC 0 (ports 0–23). The first 8 are multi-rate ports that support 100-Mbps, 1-Gbps, 2.5-Gbps, 5-Gbps, and 10-Gbps. The remaining 16 ports are GigE ports that support 10-Mbps, 100-Mbps, and 1-Gbps. • VCPs (ports 0–3 on PIC 1) support 4x1-Gbps or 4x10-Gbps or 4x25-Gbps speeds. If you convert the VCPs to network ports, ports 0 through 3 on PIC1 support 1-Gbps or 10-Gbps or 25Gbps speeds • Uplink ports (ports 0–3 on PIC 2) support 4x10-Gbps or 4x1-Gbps speeds. • EX4100-F-12P and EX4100-F-12T

Table 2: Features Supported on EX4100-48MP, EX4100-24MP, EX4100-F-12-P, and EX4100-F-12-T *(Continued)*

Feature	Description
	• Downlink ports on PIC 0 (ports 0–11). The 12 ports are GigE ports that support 10-Mbps, 100-Mbps, and 1-Gbps, • VCPs (ports 0–3 on PIC 1) support 4x1-Gbps or 4x10-Gbps speeds. If you convert the VCPs to network ports, ports 0 through 3 on PIC1 support 1-Gbps or 10-Gbps speeds • Uplink ports are multi-rate ports (ports 0–1 on PIC 2) that support 2x100-Mbps or1-Gbps speeds, 2.5-Gbps, 5-Gbps, and 10-Gbps. • Optics support. [See Hardware Compatibility Tool.] • Support for Multi-rate Power over Ethernet in EX4100 and EX4100-F switches: Apart from the switching capabilities, EX4100 switches will support Multi-rate Ethernet of 1G, 2.5G, 5G, and 10G in multi-rate switches, over existing cabling infrastructure. [See Understanding PoE on EX Series Switches.]
Junos telemetry interface	• Support for JTI Packet Forwarding Engine and Routing Engine sensor. You can use the Junos telemetry interface (JTI) and remote procedure calls (gRPC) to stream statistics from the switches to an outside collector. • Support for secure packet capture to Cloud using JTI. You can use Junos telemetry interface (JTI) to capture packets from a device and send them over a secure channel to an external collector (in the cloud) for monitoring and analysis. To use secure packet capture, include the **/junos/system/linecard/packet-capture** resource path using a Junos remote procedure call (RPC).

Table 2: Features Supported on EX4100-48MP, EX4100-24MP, EX4100-F-12-P, and EX4100-F-12-T *(Continued)*

Feature	Description
Licensing	• You need a license to use the software features on the EX4100 multigigabit switches (EX4100-48MP and EX4100-24MP) and EX4100-F-12T and EX4100-F-12P switches. To know more about licenses and supported features, see Flex Software License for EX Series Switches. To add, delete, and manage licenses, see Managing Licenses.
Security	• Support for Media Access Control security with 256-bit cipher suite. [See Understanding Media Access Control Security (MACsec).]

Table 2: Features Supported on EX4100-48MP, EX4100-24MP, EX4100-F-12-P, and EX4100-F-12-T *(Continued)*

Feature	Description
Software installation and upgrade	• Secure boot support in U-boot phase to authenticate and verify the loaded software image while also preventing software-based attack. [See Software Installation and Upgrade Guide.] • Support for DHCP option 43 suboption 8 to provide proxy server information in phone-home client. The PHC automatically starts up on the Virtual Chassis and connects to the phone-home server (PHS). The PHS responds with bootstrapping information, including the Virtual Chassis topology, software image, and configuration. The PHC upgrades each Virtual Chassis member with the new image and applies the configuration, and the Virtual Chassis is ready to go. [See Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client.] • Support for ZTP with IPv6. You can use either the legacy DHCP-options-based zero-touch provisioning (ZTP) or the phone-home client (PHC) to provision software for the EX4100 and EX4100-F switches. If the switch boots up and receives DHCP options from the DHCP server for ZTP, ZTP resumes. If DHCP options are not present, the switch attempts the PHC method. The DHCP server uses DHCPv6 options 59 and 17 and applicable suboptions to exchange ZTP-related information between itself and the DHCP client. [See Zero Touch Provisioning Overview.]

Table 2: Features Supported on EX4100-48MP, EX4100-24MP, EX4100-F-12-P, and EX4100-F-12-T *(Continued)*

Feature	Description
Timing	• Support for Precision Time Protocol (PTP) transparent clock on uplink ports connected to external MACsec PHY (EX4100-48MP and EX4100-24MP). [See Understanding Transparent Clocks in Precision Time Protocol.]
Virtual Chassis	• Support for Virtual Chassis configuration. You can interconnect EX4100-24MP, EX4100-48MP, EX4100-12T, and EX4100-12P models with other EX4100 or EX4100-F switches into a Virtual Chassis in non-mixed mode. [See Virtual Chassis Overview for Switches.]

Authentication and Access Control

- **Support for P-VLANs with egress VLAN list and 802.1X (EX2300, EX3400, EX4100, EX4100-F, EX4300, and EX4400)**—Starting in Junos OS Release 22.3R1, the listed EX Series switches support a private VLAN (P-VLAN) (with an egress VLAN ID or egress VLAN name) when 802.1X is also enabled on the port. We support IETF-defined RADIUS attributes that provide VLAN assignments and also indicate whether frames on the VLAN are tagged or untagged. This enables the network access control (NAC) server to dynamically assign VLANs on colorless ports. You can make the VLAN assignments, which are based on device profiling, on either access ports or trunk ports.

  [See Creating a Private VLAN Spanning Multiple EX Series Switches (CLI Procedure) and Configuring Colorless Ports on EX Series Switches with Aruba ClearPass Policy Manager and Cisco ISE.]

- **802.1X support on LAG interfaces (EX4400 and EX4650)** — Starting in Junos OS Release 22.3R1, 802.1X authentication is supported on LAG interfaces. 802.1X is an IEEE standard for port-based network access control that authenticates users attached to a LAN port. It blocks all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the RADIUS authentication server.

Chassis

- **Resiliency support for EX4100-F-48P, EX4100-F-48T, EX4100-F-24P, and EX4100-F-24T**—Resiliency support for inter-integrated controller (I2C), disk failure, and disk health.

Dynamic Host Configuration Protocol

-

EVPN

- **Fast reroute for egress link protection in EVPN-VXLAN multihoming environments (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T)**—Starting in Junos OS Release 22.3R1, you can enable fast reroute egress link protection (ELP) on multihoming peer provider edge (PE) devices with EVPN-VXLAN. Remote sources load balance traffic toward a multihomed customer edge (CE) device by distributing portions of the traffic among the multihoming peer PE devices. This feature minimizes load-balanced traffic loss when a peer PE device's link to the CE device goes down. The PE device creates a backup VXLAN tunnel called an ELP tunnel. The device uses the ELP tunnel to reroute its portion of the load-balanced traffic to another peer PE device. The device redirects load-balanced traffic on the ELP tunnel until the source routing table converges and the source starts sending the traffic only to the other peer PE devices.

  [See Fast Reroute for Egress Link Protection with EVPN-VXLAN Multihoming.]

Interfaces

J-Web

- **Support for EX4400 switches (EX Series)**—Starting in Junos OS Release 22.3R1, you can configure, monitor, and manage EX4400 switches by using J-Web. To configure the EX4400 switch, you must connect the Ethernet cable from the PC's Ethernet port to the port labeled **CON** on the switch's rear panel. The chassis viewer on the Dashboard page supports both the standalone device view and the Virtual Chassis configuration view (graphical view of each member switch).

  [See Dashboard for EX Series Switches and Connecting and Configuring an EX Series Switch (J-Web Procedure).]

Licensing

VLANs

-

Additional Features

We've extended support for the following features to these platforms.

- **Certificate-based authentication and encryption for MACsec** (EX4300-MP, EX4400, EX4400-MP, EX4650, and EX4650-VC)

  [See Understanding Media Access Control Security (MACsec).]

- **EVPN Type 2 and Type 5 route coexistence in edge-routed bridging (ERB) overlay EVPN-VXLAN fabrics** (EX4300-MP and EX4400-48MP)

  [See EVPN Type 2 and Type 5 Route Coexistence with EVPN-VXLAN.]

- **MAC-VRF instances with EVPN-VXLAN** (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T).

  Support for the `mac-vrf` instance type includes `vlan-based`, `vlan-aware`, and `vlan-bundle` service types for EVPN unicast routes only.

  [See MAC-VRF Routing Instance Type Overview, mac-vrf, and service-type.]

- **Optimized intersubnet multicast (OISM) in an EVPN-VXLAN fabric** (EX4300-48MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T).

  Support includes:

  - OISM server leaf role only.
  - EVPN instances configured in the default switch instance with a VLAN-aware service model only.
  - IGMPv2 with IGMP snooping.

  [See Optimized Intersubnet Multicast in EVPN Networks.]

- **Precision Time Protocol (PTP) transparent clock** (EX4400-48F and EX4400-24T)

  [See PTP Transparent Clocks , e2e-transparent, and show ptp global-information.]

- **Supported transceivers, optical interfaces, and direct attach copper (DAC) cables**. Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update this tool and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

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

General Routing

- OpenConfig container names for Point-to-Multipoint per interface ingress and egress sensors are modified for consistency from "signalling" to "signaling".

MPLS

- **Display flexible algorithm information for SRv6 locators in TED database**—Use the `show ted database extensive` command to view the metric, flags, and flexible algorithm information associated with a SRv6 locator. Prior to this release, this information was not included in the TED database.

  [See show ted database.]

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.

Platform and Infrastructure

- On EX4650 switches, Junos OS does not support the unified ISSU if there is a change in the Cancun versions of the chipset SDKs between the releases. This is a product limitation as change in the Cancun firmware leads to the chip reset and hence ISSU gets impacted. The Cancun versions in the chipset SDKs should be the same between two JUNOS OS releases for ISSU to work. PR1634695
- On EX4100 switches, the input pps, bps, and byte counters gets displayed as 0 for some ports while traffic runs without any issues. The interface status gets cleared for 0 to 23 seconds and not cleared for 24 to 47 seconds after interface flaps. This is a cosmetic issue related to display and has and no functional impact. PR1657995

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.

Forwarding and Sampling

- When you configure the `fast-lookup-filter` statement with a match that is not supported in the FLT hardware, traffic might be lost. PR1573350

Platform and Infrastructure

- On EX4400-48MP devices, the VM proccess generates core files and VC might split with multicast scale scenario. PR1614145
- When you add VLAN as an action for the changing VLAN in both ingress and egress filters, the filter does not get installed. PR1362609
- On EX4300-MPs devices, the runt, fragment, and jabber counters does not get incremented. PR1492605
- On EX4300-48MP device, if you enable POE, a primary Routing Engine might reconnect that might impact traffic. PR1499771
- Pause frames counter do not get incremented when pause frames are sent. PR1580560
- On EX4400 family of devices, sometimes login prompt does not get displayed after the login session ends. PR1582754
- In rare circumstances, when the routing-engine switchovers, the routing protocol daemon in former active routing-engine (new backup routing-engine) might restart with a core file while in process of being terminated. PR1589432
- Interop for 1G interfaces between EX4100 SKUs and ACX5448/ACX5448-M/D, and MX480 will not work. PR1657766
- The EX4100 devices, the MACsec interface statistics of the encrypted or decrypted bytes does not get updated properly after a certain value. PR1658584
- The EX4600 devices, Virtual Chassis goes in to the `Unstable` state for 3 to 7 minutes that causes traffic loss. PR1661349
- On EX92XX devices with the EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) scenario, the DHCP (Dynamic Host Configuration Protocol) packets from the client get dropped while tunneling to the EVPN-VXLAN. When this happens, the packets does not reach the DHCP server and the host could not get the IP address. PR1662524
- A common display behavior across EX platforms appears and this is inline with existing platforms. Further in vty, the following log gets generates for pic 1 ports that does not support AN: `tvp_port_resource_set AN cfg not supported on Falcon core port:1/3`. PR1666227
- On EX4100 devices, delay in the CLI display for PoE commands might be observed when more POE devices with LLDP enabled (Power via MDI) are connected to the switch in a scaled environment with Perpetual POE scenarios. The LLDP PD requested power for all the ports are processed for each of the connected PDs, however the values in CLI display (CLI sync) might be delayed. PR1671311

- When system gets rebooted or image gets upgraded, the following log might get generated during shutdown time and it is an harmless log: `BCM Error: API bcm_plp_mode_config_set(phy_name, phy_info, speed, intf_type, r_clk, if_mode, aux) at tvp_bcm_mgig_tx_enable_set:616 -> -8`

  When system comes up again, there will be no functional impact. PR1678440

- On a continuous switch reboot trigger and when the switch boots back, sometimes a vmcore process might generate a core file. PR1672731

- EX4100 and EX4100-F Virtual chassis: Non-existing PIC ports (e.g. PIC0:PORT100, PIC2:PORT102) while running the jvision query. PR1681673

- If you insert the 1G optic on the uplink ports of EX4100-24mp,EX4100-48p, EX4100-48t, EX4100-24p, and EX4100-24t SKUs, the activity LED gets lit irrespective of link in the `Present` or `Up` status. PR1682633

- EX4100 and EX4100-F series: The secondary console (USB-C type) does not show the boot logs. User will get the login prompt once the device boots up with the Junos OS. PR1684032

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.

Infrastructure

- On ARM64 platforms such as EX4100 devices, if a live vmcore gets attempted to be created, the DUT might get stuck and reboot. PR1656625

Layer 2 Ethernet Services

- DHCP packets might not be sent to the clients when you reconfigure `forward-only` under the routing instance. PR1651768

Network Management and Monitoring

- Memory might leak in eventd leak during GRES. PR1602536
- The snmpd process might crash if the SNMP timeouts. PR1666548

Platform and Infrastructure

- Traffic gets dropped after chassis-control restart when filter gets attached. PR1615548
- GARP reply does not update the ARP entry even though you configure the gratuitous-arp-reply option. PR1644616
- IRACL filters more than 64 might not work on the IRB units. PR1653216
- The dc-pfe process might crash due to the VCCP flap. PR1655530
- Junos upgrade might fail due to a storage issue in the `/var/tmp` directory. PR1659460
- On EX4300 devices, high CPU utilization appears with the following log message: `/kernel: %KERN-3: i802_3_slow_recv_input:oam/esmc PDU dropped` PR1661332
- Traffic flow gets affected as interfaces gets removed from VLAN. PR1675861
- On EX4300 and EX4300 Virtual Chassis, the fxpc process crash might. PR1675977
- The EX2300 devices might unexpectedly drop VOIP VLAN traffic after reboot. PR1633883

- IPv6 route advertisement sent on management interfaces might cause other devices to fail to get the DHCVP6 address. PR1635867
- DHCP snooping table might fail on all Junos platforms to populate MAC address after a VLAN change. PR1637380
- With SFP+-10G-CU3M DAC, link is up on EX4100-48P devices even though admin is down on peer. PR1640799
- On EX4100 devices, the class-of-service buffer-size exact configuration. PR1644355
- On EX4300, EX3400, and EX2300 devices in Virtual Chassis (VC) scenario, traffic loop might occur due to STP ports not created in the new primary Routing Engine after switchover due to reboot of the primary Routing Engine. PR1647000
- DHCP traffic might be dropped when you enable DHCP-security and RTG. PR1647209
- On EX4100 devices, non existing `et-*` interfaces details gets exported for PIC 2 for JTI server. PR1647661
- On EX4100 Virtual Chassis, ping does not work for some IRBs after the primary reboot and traffic loss occurs. PR1648310
- On EX4100 devices, junos telemetry interface FAN and power supply names do not match with CLI . PR1648739
- The Virtula Chassis port might not be formed automatically. PR1649338
- L2PT configuration on a transit switch in a Q-in-Q environment breaks L2PT. PR1650416
- On EX9251 devices, reboot reason gets displyed as `0x2000:hypervisor reboot` instead of `0x4000:VJUNOS reboot` when you reboot Junos OS. PR1651721
- On EX4100 devices, incorrect trap gets generated after removal of fan0 in FPC4. PR1652388
- The inner tag (C-tag) value might get modified to zero for egress traffic when the inner tag values are copied to the outer tag (S-tag). PR1652976
- L2PT might not work for the aggregated Ethernet interfaces in the Q-in-Q environment. PR1653260
- On EX4100 devices, enabling port beacon led functionality not working using port-range. PR1653426
- Additional debug logs might get printed onto device console, when device boots from a bootable USB. PR1653499
- On EX4100 devices, for port in 0-23 with 100m/10m speed applied AN parameters and link-mode displays HD while in the Paket Forwarding Engine link-mode displays as full-duplex. PR1654671

- Port mirroring traffic does not get flooded on the expected interfaces. PR1654812
- On EX4100 devices, partial traffic drops on the Virtual Chassis after the Routing Engine switchovers from primary to back up with NSR/NSB. PR1655052
- The egress traffic does not get tagged properly in a L2PT scenario. PR1655511
- Few EX device does not generate huge ICMPv6 messages. PR1655654
- All Slaac-snooping entries learnt on an IFL gets deleted when an IFBD gets deleted such that IFL is member of more than 1 VLANs. PR1655913
- Filter-Based Forwarding filter might not work as expected. PR1656117
- The interface might not come up. PR1656540
- On EX4100 devices, half-duplex configuration does not get applied on interfaces for members fpc 1 and above, applied only for member 0 interfaces. PR1656587
- On EX4400 devices, an incorrect PEM alarm gets raised. PR1658049
- Port or MAC gbp tags might not be carried forward to the spine. PR1659384
- Packet count gets displayed as 0 for some interfaces in when you use the `monitor interface traffic` command. PR1661617
- On EX4400-48MP devices, link activity LEDs on ports 0-35 are always lit. PR1662288
- The fxpc process might crash with the RPF check enabled. PR1662508
- SSH traffic might be affected when you use the filter log action. PR1663126
- MAC address learning failure and traffic loss might be observed on VXLAN enabled ports with native-VLAN configured. PR1663172
- MAC addresses learned on the RTG interface does not aging out. PR1664955
- MAC-IP bindings for IPv4 (ARP) and IPv6 (ND) might not be processed for IRB interfaces in an EVPN scenario. PR1665828
- High numbers of PDs connected might result in high CPU utilization. PR1667564
- Shaping-rate does not take 20 bytes of overhead into account. PR1667879
- On EX3400 devices, MAC radius authentication without restrict option updates the authenticated VLAN information before the client authentication. PR1668144
- The chassisd memory gets corrupted and the chassisd gets crashed. PR1672039

- VLAN translation programming gets deleted from the Packet Forwarding Engine upon deleting the member interface for LAG. PR1676772
- The `PRIMARY_TIMEOUT errors/auto-ttrace` error message gets generated when the DHCP traffic rate goes above the DHCP DDoS threshold. PR1647532
- DHCP binding fails for the clients (Clients connected on an aggregated Ethernet interface with 2 or more VLANs) on a VLAN where dhcp-security is not configured. PR1679094

Virtual Chassis

- On EX4600 and EX4650 devices, line card might be disconnected from Virtual Chassis post primary Routing Engine reboot. PR1669241

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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

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

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

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

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 3: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Junos OS Release Notes for JRR Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for the JRR Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

Learn about new features introduced in this release for JRR Series Route Reflectors.

Routing Protocols

- **Strip and replace BGP private-AS path (ACX710, JRR200, MX480, PTX10001, QFX5220, and QFX10003)**—In Junos OS Release 22.3R1, we have introduced the `strip-as-path` policy option that removes the incoming autonomous system (AS) path as part of the import policy for a BGP session and replaces the received autonomous system (AS) path with the receiving router's local AS number

for the receiving session. Note that the local AS number may be different from the number configured under `autonomous system` in the `[edit routing-options]` hierarchy.

If you need to normalize externally injected routes, you can use this policy option for the incoming autonomous system (AS) path so that it may be used similarly to routes that originate solely within the fabric. The new `strip-as-path` policy option has no impact on the BGP export policy.

You can configure the `strip-as-path` option under `policy-options then` clause:

```
set policy-options policy-statement do-strip term a then strip-as-path
```

[See Autonomous Systems for BGP Sessions.]

What's Changed

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

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

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

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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

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

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

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

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

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)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for Juniper Secure Connect. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for Juniper Secure Connect.

Platform and Infrastructure

- **Support for multidevice user access (Juniper Secure Connect)**—Starting in Junos OS Release 22.3R1, end users can now connect from multiple devices at the same time. To enable multi device user access, you must configure the `set security remote-access profile` *`profile-name`* `options multi-access` command.

  To configure multidevice user access, ensure you satisfy the following prerequisites:

  - Secure Connect client version is supported.
  - Each of the remote devices (computers or smart devices) has a unique hostname.

  You can clear all the IKE associations of a user using the `clear security ike active-peer aaa-username` *`user-name`* command.

  [See External User Authentication (CLI Procedure), clear security ike active-peer aaa-username, show security ipsec vpn vpnname ike idle time , Licenses for Juniper Secure Connect, and clear security ike active-peer aaa-username.]

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R1 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.

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for the Junos Fusion for enterprise. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R1 for Junos fusion for enterprise.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R1 for Junos Fusion for Enterprise.

Known Limitations

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

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

Open Issues

There are no known issues in hardware or software in this release for Junos Fusion for enterprise.

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

Resolved Issues

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

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading Junos OS on an Aggregation Device

When upgrading or downgrading Junos OS for an aggregation device, always use the `junos-install` package. Use other packages (such as the `jbundle` package) only when so instructed by a Juniper Networks support representative. For information about the contents of the `junos-install` package and details of the installation process, see the Installation and Upgrade Guide.

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

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

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the `juniper.conf` and `ssh` files), might be removed. To preserve the stored files, copy them to another system

before upgrading or downgrading the routing platform. See the Junos OS Administration Library.

To download and install Junos OS:

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

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

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

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

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

5. Select the **Software** tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

10. Install the new `junos-install` package on the aggregation device.

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

Customers in the United States and Canada, use the following commands, where *n* is the spin number.

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

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

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

Replace *source* with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

Preparing the Switch for Satellite Device Conversion

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Switch

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence,

you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 5: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Downgrading Junos OS

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

NOTE: You cannot downgrade more than three releases.
For more information, see the Installation and Upgrade Guide.

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

Junos OS Release Notes for Junos Fusion for Provider Edge

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for Junos Fusion for provider edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R1 for Junos Fusion for Provider Edge.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R1 for Junos Fusion for Provider Edge.

Known Limitations

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

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

Open Issues

There are no known issues in hardware or software in this release for Junos Fusion for provider edge.

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

Resolved Issues

There are no resolved issues in Junos OS Release 22.3R1 for Junos Fusion for provider edge.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading an Aggregation Device

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

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

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

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the `juniper.conf` and `ssh` files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. See the Installation and Upgrade Guide.

The download and installation process for Junos OS Release 21.1R1 is different from that for earlier Junos OS releases.

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

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

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

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

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

5. Select the **Software** tab.

6. Select the software package for the release.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new `jinstall` package on the aggregation device.

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

Customers in the United States and Canada, use the following commands.

- For 64-bit software:

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

```
user@host> request system software add validate reboot source/jinstall64-21.1R1.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.1R1.SPIN-domestic-signed.tgz
```

All other customers, use the following commands.

- For 64-bit software:

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

```
user@host> request system software add validate reboot source/jinstall64-21.1R1.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.1R1.SPIN-export-signed.tgz
```

Replace *source* with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 21.1R1 `jinstall` package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the `jinstall` package that corresponds to the previously installed software.

Upgrading an Aggregation Device with Redundant Routing Engines

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

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine and save the configuration change to both Routing Engines.
2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.

3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.
4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

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

Preparing the Switch for Satellite Device Conversion

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

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

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

Customers with EX4300 switches, use the following command:

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

Customers with QFX5100 switches, use the following command:

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

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

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

2. Clear the device:

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Device

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

NOTE: If the satellite device is a QFX5100 switch, you need to install a PXE version of Junos OS. The PXE version of Junos OS is software that includes *pxe* in the Junos OS package name when it is downloaded from the Software Center—for example, the PXE image for Junos OS Release 14.1X53-D43 is named install-media-pxe-qfx-5-14.1X53-D43.3-signed.tgz . If the satellite device is an EX4300 switch, you install a standard jinstall-ex-4300 version of Junos OS.

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

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

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

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

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

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

5. Review and accept the End User License Agreement.

6. Download the software to a local host.

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

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

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

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

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

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

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

9. Commit the configuration.

   To commit the configuration to both Routing Engines:

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

   Otherwise, commit the configuration to a single Routing Engine:

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

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

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

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

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

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

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

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

11. Wait for the reboot that accompanies the software installation to complete.
12. When you are prompted to log back into your device, uncable the device from the Junos fusion topology. See Removing a Transceiver from a QFX Series Device or Remove a Transceiver, as needed. Your device has been removed from Junos fusion.

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

Upgrading an Aggregation Device

When you upgrade an aggregation device to Junos OS Release 21.1R1, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

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

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

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

Downgrading from Junos OS Release 22.3

To downgrade from Release 22.3 to another supported release, follow the procedure for upgrading, but replace the 21.1 `jinstall` package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for MX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for the MX Series routers.

What's New in 22.3R1-S1

IN THIS SECTION

Learn about new features or enhancements to existing features in Junos OS Release 22.3R1-S1 for the MX Series routers.

EVPN

- **Overlay and CE-IP ping and traceroute support for EVPN-VXLAN (MX304)**—Starting in Junos OS Release 22.3R1-S1, you can perform ping and traceroute operations within an EVPN-VXLAN overlay or to a specific customer edge [CE] device IP address (CE-IP) across an EVPN-VXLAN overlay. Overlay ping and traceroute, and CE-IP ping and traceroute are used for fault detection and isolation in overlay networks.

  [See ping overlay.]

  [See traceroute overlay.]

  [See ping ce-ip.]

  [See traceroute ce-ip.]

Junos Telemetry Interface

- **Support for logical interface-set sensors (MX304 with Trio chipset EA, ZT, and YT-based fixed systems and modular systems line cards)**—Starting in Junos OS Release 22.3R1-S1, Junos telemeytry interface (JTI) supports logical interface (IFL)-set sensors. The sensors stream queue statistics using Juniper proprietary gRPC and gRPC Network Management Interface (gNMI) or by means of UDP. Zero suppression (suppressing zero values in statistics from streamed data) is also supported.

  [See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface) and sensor (Junos Telemetry Interface).]

MPLS

- **Support for ingress and transit chained CNHs for BGP-LU IPv4 (MX304)**—Starting in Junos OS Release 22.3R1-S1, you can configure chained composite next hops (CNHs) for devices handling ingress or transit traffic in the network. We've added support for the following options on select MX Series routers:

  - BGP Labeled Unicast (BGP-LU) for IPv4 on the ingress router—`set routing-options forwarding-table chained-composite-next-hop ingress labeled-bgp inet`

  - BGP-LU on the transit router—`set routing-options forwarding-table chained-composite-next-hop transit labeled-bgp`

  You can also configure class of service (CoS) and define rewrite rules for ingress and transit chained CNHs for BGP-LU.

  [See labeled-bgp, chained-composite-next-hop, and ingress (Chained Composite Next Hop).]

Licensing

- **Juniper Agile Licensing (MX304)**—Starting in Junos OS Release 22.3R1-S1, the MX304 router supports Juniper Agile Licensing.

  Juniper Agile Licensing provides simplified and centralized license administration and deployment. You can use Juniper Agile Licensing to install and manage licenses for hardware and software features.

  Juniper Agile Licensing supports soft enforcement and hard enforcement of hardware and software feature licenses.

  - With soft enforcement, if you configure a feature without a license, Junos OS displays a warning when you commit the configuration. However, the feature remains operational. In addition, Junos OS generates periodic alarms indicating that you need the license to use the feature. You can see the list of alarms at System Log Explorer.

  - With hard enforcement, if you configure a feature without a license, Junos OS displays a warning when you commit the configuration. The feature is not operational until the license is installed. In addition, Junos OS generates periodic syslog messages indicating that you need the license to use the feature. You can see the list of syslog messages at System Log Explorer.

Table 7: Licensed Features on MX304 Device

License Model	Use Case Examples or Solutions	Features	Scale
Standard	Basic Layer 2 features	Bridging with port and single-level VLAN (dot1Q), LAG, and xSTP	–

Table 7: Licensed Features on MX304 Device *(Continued)*

License Model	Use Case Examples or Solutions	Features	Scale
Advanced	Transport	• Includes standard features • IP routing, IGP (OSFP and IS-IS), IP-FRR, PIM variants, and IGMP • Internet eBGP peering, BGP multihoming (add path and multipath), EPE, and BGP PIC • BGP flow specification • All Layer 2 services—E-Line (Layer 2 VPNs, Layer 2 circuit, EVPN VPWS, EVPN FXC), E-LAN (bridging, H-VPLS, EVPN, and IRB), E-Tree (H-VPLS, EVPN, and IRB), Layer 2 multicast (snooping included) • All MPLS transport—LDP, RSVP-TE, segment routing, SR-TE, and MPLS-FRR (including TI-LFA) • IP fabrics (MPLS-over-UDP, VXLAN, and IP-in-IP) • GRE	32 IP VPNs 8 multicast VPNs

Table 7: Licensed Features on MX304 Device *(Continued)*

License Model	Use Case Examples or Solutions	Features	Scale
		• Streaming telemetry and SNMP • Policers, ACLs, J-Flow, port mirroring, and per VLAN queuing • PWHT for Layer 2 • Timing (all variants) • OAM—BFD, Ethernet CFM or LFM, MPLS or segment routing (ping and traceroute), services OAM, RPM, and TWAMP	
Premium	Services	• Includes advanced features • High-scale IP-VPNs • IP fabrics (SRv6 and SRm6) • PWHT for Layer 3 VPNs • Inline NAT and inline MDI • 1:1 inline J-Flow	32+ IP VPNs 8+ multicast VPNs

[See Flex Software License for MX and Managing Licenses.]

Subscriber Management and Services

- **Support for accurate transmit logical interface statistics on pseudowire subscriber logical interface (MX304)**—Starting with Junos OS Release 22.3R1-S1, we support accurate transmit logical interface

statistics on the services side of an MPLS pseudowire subscriber logical interface. These statistics represent actual transmit data instead of the load statistics that the router provides for the pseudowire subscriber service logical interfaces.

[See show interfaces.]

Additional Features for S1

What's New in 22.3R1

IN THIS SECTION

Learn about new features or enhancements to existing features in Junos OS Release 22.3R1 for the MX Series routers.

Class of Service

- **HCoS support for transport slices (MX Series)**—Starting with Junos OS Release 22.3R1, MX Series devices support hierarchical CoS (HCoS) for transport slices. You can configure up to three levels of HCoS for transport slices:
  - Physical interface (Level 1)
  - Individual slices (Level 2)
  - Eight queues per slice (Level 3)

  You can assign a traffic control profile (TCP) to a slice by setting `slice` *`slice-name`* `output-traffic-control-profile` *`tcp-name`* at the `[edit class-of-service interface` *`interface-name`*`]` hierarchy level.

  [See slice (CoS Interfaces).]

- **HCoS support for per-slice statistics (MX Series)**—
  Starting with Junos OS Release 22.3R1, you can view hierarchical CoS (HCoS) per-slice statistics for a physical interface on an MX Series device. To see the per-slice statistics, use the `show interfaces queue` *`interface-name`* `slice` *`slice-name`* command.

  [See show interfaces queue .]

Chassis

- **MX10004 Support for SF2 (JNP10008-SF2) Resiliency** on MX10004 devices.
  [See MX10004 Hardware Guide.]
- **SF2 Platform Support for MX10004** that includes:
  - Platform support for switch fabric with 1 ZF ASIC (SF2) and four FPC slots.
  - FRU management support for:
    - Two fan trays, Two fan tray controllers.
    - Six SF2s (JNP10004-SF2).
    - LED and alarms for FRU.
  - Three 5.5 KW PSMs slots with AC or DC PSUs.
  - FPC and PSM power management with support for temperatures from 25C to 40C.

[See show chassis hardware, request chassis fpc, show chassis sfb, show chassis sfb errors, and MX10004 Hardware Guide.]

- **Fabric Management Support for MX10004**, that includes:
  - New switch fabric, SF2 (JNP10004-SF2) with single ASIC.
  - Six fabric boards, and four line card slots.
  - Dual RCB (RE + CB) boards in master and backup roles.
  - Master Control Board (CB) (model numbers: JNP10K-RE1, JNP10K-RE1-128 or JNP10K-RE1-LT) that controls all components in the system, including the SF2.

  [See No Link Title, request chassis fpc, request chassis sfb, show chassis fabric plane, show chassis fabric fpcs, show chassis fabric summary, show chassis alarms, show chassis fabric stream-info.]

EVPN

- **EVPN-VPWS over SRv6 underlay (MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, and MX10008)**—Starting in Junos OS Release 22.3R1, you can configure a single-active or an all-active multihomed Ethernet VPN–virtual private wireless service (EVPN-VPWS) network using Segment Routing over IPv6 (SRv6).

  To enable EVPN-VPWS over SRv6, configure the following:

  1. Include the `end-dx2-sid` statement at the `[edit routing-instances` *`instance-name`* `protocols evpn source-packet-routing srv6 locator name]` hierarchy level or the `[edit routing-instance` *`routing-instance-name`* `protocols evpn interface` *`interface-name`*`]` hierarchy level for the `evpn-vpws` instance type.
  2. Include the `enhanced-ip` statement at the `[edit chassis network-services]` hierarchy level.
  3. Enable `advertise-srv6-service` and `accept-srv6-service` in the `[edit protocols bgp group` *`name`* `family evpn]` hierarchy.

     [See Configuring VPWS with EVPN Signaling Mechanisms and Understanding SRv6 Network Programming and Layer 3 Services over SRv6 in BGP.]

- **Overlay and CE-IP ping and traceroute support for EVPN-VXLAN (MX240, MX480, MX960, MX2010, MX2020, and MX10008)**—Starting in Junos OS Release 22.3R1, you can perform ping and traceroute operations within an EVPN-VXLAN overlay or to a specific customer edge [CE] device IP address (CE-IP) across an EVPN-VXLAN overlay. Overlay ping and traceroute, and CE-IP ping and traceroute are used for fault detection and isolation in overlay networks.

  [See ping overlay.]

  [See traceroute overlay.]

[See ping ce-ip.]

[See traceroute ce-ip.]

Hardware

- **New MX10004 Universal Routing Platform (MX Series)**—

  In Junos OS Release 22.3R1, we introduce the MX10004 router as the most compact, high-density, and power-efficient modular device in the MX10000 line of routers. This next-generation edge, metro aggregation, and peering platform is only 7 U in height and is designed for space-constrained facilities. Like the larger MX10008 router, the MX10004 supports Juniper's 400GbE architecture with inline Media Access Control Security (MACsec) on all ports for point-to-point security on Ethernet links.

  To install the MX10004 router hardware and perform initial software configuration, routine maintenance, and troubleshooting, see MX10004 Universal Routing Platform Hardware Guide.

Table 8: Feature Support on MX10K-LC9600

Feature	Description
Chassis	• Support for VM host. [See VMHost Overview (Junos OS).] • • Support for new ZF-based switch fabric 2 (SF2) • Fabric support for line cards LC2101, LC480, and LC9600 Fabric management and Doon RCB support for MX10004 with line cards and Junos OS version . [See show chassis environment sfb • **SF2 Platform Support for MX10004** that includes: • Platform support for switch fabric with 1 ZF ASIC (SF2) and four-slots. • FRU management support for: • Two fan trays and two fan tray controllers. • Three SFBs. • LED and alarms for FRU. • Three 5.5 KW PSM slots with AC or DC PSUs. • FPC and PSM power management with support for temperatures from 25C to 40C. [See show chassis alarms, show chassis sfb , show system firmware] • • Platform Resiliency Support for MX10004, that includes: • Resiliency for FRUs and new SF2 (switch fabric) • Support for NSR, routing engine switchover of SF2 (GRES) [See MX10004 Hardware Guide and Fabric-Plane-Management-on-MX10004-Devices] .]
Class of service (CoS)	• Support for forwarding CoS. [See Understanding Class of Service.]

Table 8: Feature Support on MX10K-LC9600 *(Continued)*

Feature	Description
Distributed denial-of-service	• Support for distributed denial-of-service (DDoS) protection . [See Control Plane Distributed Denial-of-Service (DDoS) Protection Overview.]
Firewall filter	• Firewall filter processing. [See Understanding Firewall Filter Match Conditions.]

Hardware	• New JNP10004-SF2 Switch Fabric Board (SFB). The ZF ASIC-based JNP10004-SF2 SFB makes up the MX10004 switching plane to provide fabric interconnect for the custom silicon line cards with 480-Gbps, 2.4-Tbps, and 9.6-Tbps throughput. The MX10004 supports six SFBs. With all six SFBs and all four MX10K-LC9600 line cards installed, the MX10004 has a net switching capacity of 38.4 Tbps. Each SFB has four connectors that correspond to a matching connector on one of the four line cards. Depending on the type of line card used, you can have either 5+1 fabric card redundancy or no redundancy.
	
	• SF2 platform support, including:
	
	  • Platform support for switch fabric with 1 ZF ASIC (SF2) and four slots
	
	  • FRU management support for:
	
	  • Two fan trays, two fan tray controllers
	
	  • Three SF2 SFBs (JNP10004K-SF2)
	
	  • LED and alarms for FRU
	
	  • Slots for three 5.5-kW PSMs with AC or DC PSUs
	
	  • FPC and PSM power management with support for temperatures from 25° C through 40° C
	
	  •
	
	• Support for SF2 (JNP10004-SF2) resiliency.

Table 8: Feature Support on MX10K-LC9600 *(Continued)*

Feature	Description
Interfaces	• Interface support. The MX10004 supports the MX10K-LC2101, MX10K-LC480, and MX10K-LC9600 line cards with throughput of 2.4 Tbps, 480 Gbps, and 9.6 Tbps, respectively. You can configure the port speed at the [`edit chassis`] hierarchy level. [See Port Speed.] • Support for load balancing. [See Understanding Per-Packet Load Balancing.]
Static tunnel	• Support for static tunnel. [See Tunnel Services Overview.]
Junos Broadband Edge (BBE)	• Support for Junos BBE. [See Junos OS Enhanced Subscriber Management.]

Table 8: Feature Support on MX10K-LC9600 *(Continued)*

Feature	Description
Junos telemetry interface	• Telemetry support for fabric sensors. [See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).] • Support for chassis management error (cmerror) telemetry statistics. [See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface) and Telemetry Sensor Explorer.] • Support for platform sensor optics. [See Telemetry Sensor Explorer.] • Support for platform and alarm sensors. [See Telemetry Sensor Explorer.] • Support for physical, logical, and Ethernet interface statistics. [See Telemetry Sensor Explorer.} • Sensor support for transceiver diagnostics based on the OpenConfig data model **openconfig-platform-transceiver.yang**, version 0.5.0. [See Telemetry Sensor Explorer.]
Layer 2 features	• Layer 2 features support. [See Configuring Q-in-Q Tunneling and VLAN Q-in-Q Tunneling and VLAN Translation, Understanding Layer 2 Bridge Domains, Understanding Layer 2 Learning and Forwarding, Introduction to OAM Connectivity Fault Management (CFM), Enabling MAC Accounting for a Router or a Bridge Domain, LLDP Overview, Configuring Aggregated Ethernet LACP, and EVPN Overview.]
Layer 3 features	• Forwarding Layer 3 routing features support. [See Understanding OSPF Configurations, BGP Overview, z, and Bidirectional Forwarding Detection (BFD).] • Layer 3 features support. [See MPLS Overview, Multicast Overview, and Understanding Next-Generation MVPN Control Plane.]

Table 8: Feature Support on MX10K-LC9600 *(Continued)*

Feature	Description
Network management and monitoring	• Support for port mirroring. [See Configuring Port Mirroring on M, T MX, ACX, and PTX Series Routers.]
Timing synchronization	• Support for timing synchronization and link aggregation group (LAG). See Time Management and Synchronization Overview and Configuring Multichassis Link Aggregation on MX Series Routers.] • Support for PTP G8275.1 profile. See Configuring G.8275.1 Profile.]
Services applications	• Support for inline services, including: • Inline NAT—NAT44 and NPTv6 • Inline softwires—MAP-E and 6rd • Inline active flow monitoring • Inline monitoring services • Inline video monitoring • FlowTapLite [See Inline NAT, Configuring Mapping of Address and Port with Encapsulation (MAP-E), Configuring Inline 6rd, Understand Inline Active Flow Monitoring, Inline Monitoring Services Configuration, Understanding Inline Video Monitoring, and Configuring FlowTapLite.]
Subscriber management and services	LC2101 and LC480 line cards support Multi-Access User Plane/Wireless CUPS. [See Multi-Access User Plane Overview.]

Interfaces

Junos Telemetry Interface

- **Support for AGF sensors (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 22.3R1, you can use Access Gateway Function (AGF)-specific sensors in Junos telemetry interface (JTI) to collect data on AGF interactions. Use the data to gain early detection to problems occurring in real time, optimize traffic engineering, and improve the design of your network.

  [See Telemetry Sensor Explorer.]

- **BGP policy sensor upgrade (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10002, and vRR)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports data model **openconfig-bgp-policy.yang** version 6.0.2 (upgraded from version 4.0.1). JTI also supports new BGP policy sensors.

  [See Telemetry Sensor Explorer.]

- **Packet Forwarding Engine DDoS sensor support with JTI (MX960, MX10004, MX10008 and MX2020 operating with Module Port Concentrator (MPC) 10 or 11 or the LC9600 Line Card)**—Starting in Junos OS Release 22.3R1, JTI supports distributed denial-of-service (DDoS) telemetry sensors. To stream DDoS statistics from a device to a collector, include the resource path **/junos/system/linecard/ddos/**) in a subscription. You can stream statistics using UDP (native) or Juniper proprietary gRPC and gNMI. This feature supports the Openconfig data model **junos/ui/openconfig/yang/junos-ddos.yang**.

  Currently, there are 227 packet types for DDoS. To maintain a reasonably sized data stream, data is exported for all protocols that have traffic using the zero-suppression model.

  [See sensor (Junos Telemetry Interface) and Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).]

- **Support for logical interface-set sensors (MX204, MX240, MX480, MX960, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016 with Trio chipset EA, ZT, and YT-based fixed systems and modular systems line cards)**—Starting in Junos OS Release 22.3R1, Junos telemeytry interface (JTI) supports logical interface (IFL)-set sensors. The sensors stream queue statistics using Juniper proprietary gRPC and gRPC Network Management Interface (gNMI) or by means of UDP. Zero suppression (suppressing zero values in statistics from streamed data) is also supported.

  [See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface) and sensor (Junos Telemetry Interface).]

- **Support for MPLS RSVP-TE sensors (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, and PTX10002)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports data model **openconfig-mpls-rsvp.yang** version 4.0.0. It supports new RSVP-TE sensors.

  [See Telemetry Sensor Explorer.]

- **Support for MPLS OpenConfig configuration and sensors (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, and PTX10002)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports the following data models:

  - **openconfig-mpls.yang** version 3.2.2
  - **openconfig-mpls-types.yang** version 3.2.1
  - **openconfig-mpls-te.yang** version 3.2.2
  - **openconfig-mpls-static.yang** version 3.2.2

  JTI supports the following OpenConfig configurations:

  - MPLS global
  - MPLS `named-explicit-path`
  - MPLS tunnels

  JTI supports the following state groups:

  - MPLS tunnels
  - MPLS `named-explicit-path`
  - MPLS static `label-switched-path`
  - MPLS-TE interface attributes
  - MPLS tunnel state counters (dependent on the Packet Forwarding Engine)

  [See Telemetry Sensor Explorer and Mapping OpenConfig MPLS Commands to Junos Configuration.]

- **INITIAL_SYNC enhancement for FIB streaming (MX240, MX960, MX2010, MX2020, PTX1000, PTX5000, and PTX10008)**—Junos OS Release 22.3R1 introduces improved performance time for the INITIAL_SYNC of telemetry statistics. This enhancement applies to subscription requests for the top-level sensor path **/network-instances/network-instance/afts**. The INITIAL_SYNC feature gives the collector a complete view of the current state of every field on the device for that sensor path.

  [See Enabling “INITIAL_SYNC” Subscription Mode through gNMI.]

- **Sensor for LSP name of MPLS next hops (MX240, MX960, MX2020, PTX1000, and PTX5000)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports the **/network-instances/network-instance/afts/next-hops/next-hop/state/lsp-name** sensor. This sensor will stream the LSP name associated with the nexthop.

  [See Telemetry Sensor Explorer.]

- **Support for VLAN sensors (ACX5448, ACX5448-M, ACX5448-D, and ACX710 routers, EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC and EX9208 switches, MX204, MX240, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2010, MX2020, PTX10008, and PTX10016 routers and vMX)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports the data model **openconfig-vlan.yang** version 3.2.1, including sensor support to stream VLAN and MAC- limit operational states through telemetry.

  [See Telemetry Sensor Explorer.]

J-Web

Licensing

- **Support for Layer 2 and Layer 3 QoS (MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, and MX10016)**—Starting in Junos OS Release 22.3R1, the listed MX Series devices support the Layer 2 and Layer 3 QoS feature. The Layer 2 and Layer 3 QoS feature is part of the Advanced license model.

  [See Flex Software License for MX Series Routers and MPC Service Cards.]

MACsec

- **MACsec delay protection (MX10008 and MX10016)**—Starting in Junos OS Release 22.3R1, we support MACsec bounded delay protection on MX10008 and MX10016 routers.

  [See bounded-delay .]

- **Support for MACsec on logical interfaces (MX10008 and MX10016)**—Starting in Junos OS Release 22.3R1, you can transmit VLAN tags in cleartext, which allows intermediate switches that aren't MACsec aware to switch the packets based on the VLAN tags.

  [See Media Access Control Security (MACsec) over WAN.]

MPLS

- **Support for ingress and transit chained CNHs for BGP-LU IPv4 (MX204, MX240, MX480, MX960, MX2010, MX2020, MX10003, MX10008, and MX10016)**—Starting in Junos OS Release 22.3R1, you can configure chained composite next hops (CNHs) for devices handling ingress or transit traffic in the network. We've added support for the following options on select MX Series routers:

- BGP Labeled Unicast (BGP-LU) for IPv4 on the ingress router—`set routing-options forwarding-table chained-composite-next-hop ingress labeled-bgp inet`
- BGP-LU on the transit router—`set routing-options forwarding-table chained-composite-next-hop transit labeled-bgp`

You can also configure class of service (CoS) and define rewrite rules for ingress and transit chained CNHs for BGP-LU.

[See labeled-bgp, chained-composite-next-hop, and ingress (Chained Composite Next Hop).]

Network Address Translation (NAT)

- **AMS support for load balancing (MX Series)**—Starting in Junos OS Release 22.3R1, we support load balancing using the new CLI option `modulo-key` in the `set interfaces ams0 unit 1 load-balancing-options` command.

  [See Configuring Load Balancing on AMS Infrastructure.]

Network Management and Monitoring

- **Support for SRv6 traceroute (MX240, MX480, MX960, MX2008, MX10003, MX10008, and vMX)**—Starting in Junos OS Release 22.3R1, we support the traceroute mechanism for Segment Routing for IPv6 (SRv6) segment identifiers. You can use traceroute for both UDP and ICMP probes. By default, traceroute uses UDP probe. For ICMP-probe, use the traceroute command with `probe-icmp` option.

  [See .]How to Enable SRv6 Network Programming in IS-IS Networks

- **IPv6 and IPv4 multicast and unicast traffic statistics (MX240, MX480, MX960, MX2010, MX2020, MX10003, MX10008, and MX10016)**

  —Starting in Junos OS Release 22.3R1, we support input and output packets, bytes counters, and rate counters for IPv6 and IPv4 multicast and unicast traffic. This feature helps enhance the traffic statistics collection process. To enable this feature, use `detailed-transit-interface-stats enable` at the `[edit accounting-options]` hierarchy level. Use `show interfaces ge-1/2/9.0 extensive` to display the Layer 3 transit statistics.

  [See show interfaces extensive and accounting-options.]

OpenConfig

- **Support for OpenConfig VLAN model (ACX5448, MX10003, PTX10008, QFX5110, and QFX10002)**—Starting in Junos OS Release 22.3R1, we support the OpenConfig VLAN data model **openconfig-vlan.yang**, version 3.2.1. You can use paths for configuration and for streaming of operational state data.

[For operational state paths, see Telemetry Sensor Explorer. For configuration, see Mapping OpenConfig VLAN Commands to Junos Configuration.]

- **Support for OpenConfig BFD configuration and state (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, and PTX10002)**—Starting in Junos OS Release 22.3R1, we support OpenConfig configuration and state support for BFD. Use BFD telemetry data to detect failures in the forwarding path between two adjacent routers.

  [See Mapping OpenConfig Interface Commands to Junos Configuration and Telemetry Sensor Explorer.]

- **OpenConfig IS-IS configuration support (ACX5448, ACX710, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX3000, PTX10002, and PTX10003)**—Starting in Junos OS Release 22.3R1, we support IS-IS configuration using OpenConfig.

  [See Mapping OpenConfig ISIS Commands to Junos Configuration.]

Precision Time Protocol (PTP)

- **G.8275.1 profile with BITS as a frequency source in hybrid mode (MX10008 with MX10K-LC2101 line cards)**—Starting in Junos OS Release 22.2R1, you can configure BITS as a frequency source with the G.8275.1 profile in hybrid mode. G.8275.1 also supports PTP over Ethernet (PTPoE) over LAG with BITS as the frequency source. If you configure Synchronous Ethernet and BITS each as a frequency source, then based on the clock selection, either Synchronous Ethernet or BITS is chosen as the frequency source in hybrid mode.

  [See show ptp hybrid and show chassis synchronization (MX Series Router).]

Routing Policy and Firewall Filters

- **Support for MPLS label-based classification** (MX480, MX960, MX10003, MX2020)

  Starting in Junos 22.3R1, we support label-based classification to match the top label, bottom label, or the label at a specified offset from the top or bottom of the label stack of the incoming MPLS packet for MPLS family filters.

Routing Protocols

- **SSH host-key algorithm configuration enhancements (MX960)**—Starting in Junos OS Release 22.3R1, we've replaced the `system services ssh hostkey-algorithm` configuration statement with the `system services ssh hostkey-algorithm-list` statement. When you use the `hosykey-algorithm-list` statement, Junos OS uses only the specified host-key algorithms and automatically disables the rest of the algorithms.

If you do not specify any host-key algorithms, Junos OS uses the default algorithms RSA, ECDSA, and ED25519.

[See hostkey-algorithm-list.]

- **Fast lookup of origin and neighbor ASs (MX480, MX960, MX10008, PTX1000, PTX10002, PTX10008, PTX10016, QFX10008, and vRR)**—Starting in Junos OS Release 22.3R1, you can use the new `asregex-optimize` configuration statement at the `[edit policy-options defaults]` hierarchy level to perform a fast lookup of origin and neighbor autonomous systems (ASs). This optimization supports very large AS-Path regular expressions (typically as-path-group configuration) when the objective is to match neighboring ASes, or origin ASes.

  [See Improve the Performance of AS Path Lookup in BGP Policy.]

- **IS-IS flood optimization (MX960, MX2008, MX2010, MX2020, PTX10002, PTX10008, and PTX10016)**—Starting in Junos OS Release 22.3R1, you can rate-limit the IS-IS link-state PDUs that are retransmitted on parallel interfaces toward the same peer. This feature optimization prevents frequent drops in IS-IS hello protocol data units (PDUs) and subsequent adjacency reset. The optimizations also involve changes to the LSP transmission queues to avoid longer delays for frequently updated LSPs.

- **Sharding support for condition route manager (MX204 and MX480)**—Starting in Junos OS Release 22.3R1, we have added sharding support for the condition manager to fetch active route information from the main thread for conditions. The condition manager on a shard interacts with the route target Proxy client to get active route information, and the condition manager on the main thread interacts with the route target proxy server to send details to the shards. The condition manager on each shard stores active route information that is true or false for any condition and evaluates the policy (having condition) based on that information. The condition manager on the main thread continues to perform route lookup, flash mechanism operations, and the dependent route operations, such as addition or deletion, according to the existing process.

  We've updated the following command outputs:

  - `show policy condition`
  - `show policy condition detail`
  - `show policy condition` *`condition-name`*
  - `show policy condition` *`condition-name`* `detail`
  - `show policy condition rib-sharding` *`shard-name`*
  - `show policy condition detail rib-sharding` *`shard-name`*
  - `show policy condition` *`condition-name`* `rib-sharding` *`shard-name`*

- `show policy condition` *`condition-name`* `detail rib-sharding` *`shard-name`*

[See Routing Policy Match Conditions, rib-sharding, and show policy conditions.]

- **Strip and replace BGP private-AS path (ACX710, JRR200, MX480, PTX10001, QFX5220, and QFX10003)**—In Junos OS Release 22.3R1, we have introduced the `strip-as-path` policy option that removes the incoming autonomous system (AS) path as part of the import policy for a BGP session and replaces the received autonomous system (AS) path with the receiving router's local AS number for the receiving session. Note that the local AS number may be different from the number configured under `autonomous system` in the `[edit routing-options]` hierarchy.

  If you need to normalize externally injected routes, you can use this policy option for the incoming autonomous system (AS) path so that it may be used similarly to routes that originate solely within the fabric. The new `strip-as-path` policy option has no impact on the BGP export policy.

  You can configure the `strip-as-path` option under `policy-options then` clause:

  ```
  set policy-options policy-statement do-strip term a then strip-as-path
  ```

  [See Autonomous Systems for BGP Sessions.]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **SRv6 flexible algorithms in TED and BGP-LS (MX10008)**—Starting in Junos OS Release 22.3R1, we support Segment Routing for IPv6 (SRv6) flexible algorithms in traffic engineering database (TED) and BGP Link State (LS). Flexible algorithms enable routing protocols such as IS-IS and OSPF to compute paths over a network based on user-defined parameters such as calculation type, metrics, and constraints. You cannot define flexible algorithms specifically for either SR-MPLS or SRv6. If a node is participating in a flexible algorithm it would apply to both SR-MPLS and SRv6 nodes.

  [See How to Configure Flexible Algorithms in IS-IS for Segment Routing Traffic Engineering and BGP Link-State Extensions for Source Packet Routing in Networking (SPRING).]

- **BGP service route resolution over SRv6 SIDs (MX10008)**—Starting in Junos OS Release 22.3R1, we support the resolution of IPv6 routes over Segment Routing for IPv6 (SRv6) segment identifiers (SIDs) for the following prefixes:

  - Prefixes associated with the BGP extended community color attribute. You can configure the BGP transport class for resolution of IPv6 routes over the flexible algorithm locator. Note that BGP prefers the PNH or the SRv6 segment routing–traffic engineering (SR-TE) policy over the SRv6 flexible algorithm.

  - Prefixes that are not associated with the BGP extended community color attribute.

  [See BGP Classful Transport (BGP-CT) with Underlying Colored SR-TE Tunnels Overview.]

Services Applications

- **Partial reassembly of IPv4 packets for MAP-E (MX Series routers)**—Starting in Junos OS Release 22.3R1, the line cards on MX Series routers support partial reassembly of IPv4 packets for Mapping of Address and Port with Encapsulation (MAP-E). The MAP-E border relay device encapsulates the IPv4 packets from public IPv4 networks into IPv6 and then routes the packets to the MAP-E customer edge (CE) devices.

  [See Understanding Mapping of Address and Port with Encapsulation (MAP-E).]

Software Defined Networking (SDN)

- **Support for Ubuntu 20.04 in Junos node slicing (MX480, MX960, MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 22.3R1, the external server-based Junos node slicing supports Ubuntu 20.04 on the x86 servers. In Junos OS releases before Release 22.3R1, Junos node slicing supports Ubuntu 16.04. If you are currently running Ubuntu 16.04, we recommend that you upgrade your host OS to Ubuntu 20.04 before upgrading to Junos OS Release 22.3R1.

  [See Setting Up Junos Node Slicing.]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **SRv6 flexible algorithms in TED and BGP-LS (MX10008)**—Starting in Junos OS Release 22.3R1, we support Segment Routing for IPv6 (SRv6) flexible algorithms in traffic engineering database (TED) and BGP Link State (LS). Flexible algorithms enable routing protocols such as IS-IS and OSPF to compute paths over a network based on user-defined parameters such as calculation type, metrics, and constraints. You cannot define flexible algorithms specifically for either SR-MPLS or SRv6. If a node is participating in a flexible algorithm it would apply to both SR-MPLS and SRv6 nodes.

  [See How to Configure Flexible Algorithms in IS-IS for Segment Routing Traffic Engineering and BGP Link-State Extensions for Source Packet Routing in Networking (SPRING).]

- **BGP service route resolution over SRv6 SIDs (MX10008)**—Starting in Junos OS Release 22.3R1, we support the resolution of IPv6 routes over Segment Routing for IPv6 (SRv6) segment identifiers (SIDs) for the following prefixes:

  - Prefixes associated with the BGP extended community color attribute. You can configure the BGP transport class for resolution of IPv6 routes over the flexible algorithm locator. Note that BGP prefers the PNH or the SRv6 segment routing–traffic engineering (SR-TE) policy over the SRv6 flexible algorithm.

  - Prefixes that are not associated with the BGP extended community color attribute.

  [See BGP Classful Transport (BGP-CT) with Underlying Colored SR-TE Tunnels Overview.]

Subscriber Management and Services

- **Support for accurate transmit logical interface statistics on pseudowire subscriber logical interface (MX240, MX480, MX960, MX2010, MX2020, MX10008, and MX10016)**—Starting with Junos OS Release 22.3R1, we support accurate transmit logical interface statistics on the services side of an MPLS pseudowire subscriber logical interface. These statistics represent actual transmit data instead of the load statistics that the router provides for the pseudowire subscriber service logical interfaces.

  [See show interfaces.]

- **Access Gateway Function (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 22.3R1, we introduce the Access Gateway Function (AGF). AGF provides wireline traffic convergence by interworking wireline connected devices with the 5G Core (5GC). AGF is the access point for existing fixed network residential gateway (FN-RG) and is an integral part of the Junos Multi-Access User Plane solution. AGF supports the following capabilities:

  - DHCP relay and DHCPv6 stateful relay service for relay client negotiations to a DHCP server in the 5GC
  - PPPoE access to the 5GC
  - N1 proxy signaling for user equipment (UE) registration and Protocol Data Unit (PDU) session establishment procedures for FN-RG authentication, address assignment, and authorization
  - N2 signaling with the Access and Mobility Management Function (AMF)
  - N3 signaling to both an external and colocated user plane function (UPF) that supports per subscriber IP and IPv6 data connectivity to a data network
  - UE-level QoS that originate from the 5GC authorization
  - Colocation of AGF, broadband network gateway (BNG), and UPF services on a single MX Series router

  You can configure AGF services in the `[edit services agf]` hierarchy.

  [See AGF User Guide.]

- **SCTP support (MX204, MX240, MX480, MX960, and MX10003)**—In Junos OS Release 22.3R1, you can configure SCTP to connect the Access Gateway Function (AGF) with the Access and Mobility Management functions (AMFs). SCTP is a reliable connection-oriented protocol that you use for transporting message streams.

  - Multistream protocol
  - User data fragmentation
  - Chunk bundling

- Packet validation
- Multihome support

AGF creates an SCTP association to communicate with the AMFs. You can configure the SCTP association in the `[edit services agf amf]` hierarchy.

Use the `show system connections | find sctp` command to check the SCTP endpoints and associations.

Use the `show system statistics sctp` command to query the SCTP system-wide statistics.

[See AGF User Guide, show system statistics, and show system connections.]

- **Support for Multi-Access User Plane (MX10004)**—Starting in Junos OS Release 22.3R1, LC2101 and LC480 line cards support Junos Multi-Access User Plane functions.

  [See Multi-Access User Plane User Guide.]

Additional Features

We've extended support for the following features to these platforms.

What's Changed

IN THIS SECTION

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

General Routing

- OpenConfig container names for Point-to-Multipoint per interface ingress and egress sensors are modified for consistency from "signalling" to "signaling".

- For Access Gateway Function (AGF) statistics, consistency changes are implemented for specific leaf values in telemetry data to match field values in Junos CLI operational mode commands. AGF NG Application Protocol (NGAP) data streamed to a collector and viewable from the Junos OS CLI now displays "ngap-amf-stats-init-ctx-setup-failure" and Access and Mobility Function (AMF) overload state now displays "On, Off".

- **Router advertisement module status on backup Routing Engine (MX Series)**—The router advertisement module does not function in the backup Routing Engine as the Routing Engine does not send an acknowledgment message after receiving the packets. Starting in this Junos OS Release, you can view the router advertisement module information using the `show ipv6 router-advertisement` operational command.

  [See show ipv6 router-advertisement].

- **Instance type change is not permitted from default to L3VRF in open configuration (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—DEFAULT_INSTANCE is the primary instance that runs when there is no specific instance type configured in the route `set routing-options`. Any instance you explicitly configure is translated into `set routing-instance r1 routing-options`. The issue appears in translation, when you change instance type DEFAULT_INSTANCE (any instance to DEFAULT_INSTANCE) to L3VRF or L3VRF to DEFAULT_INSTANCE. As a result, such changes are not permitted. Additionally, DEFAULT_INSTANCE can only be named DEFAULT, and DEFAULT is reserved for DEFAULT_INSTANCE, therefore allowing no such changes.

- **Support for DDoS protocol (MX10008)**—We've enabled the DDoS protocol support at the **`edit system ddos-protection`** hierarchy level for MX10008 devices. In earlier releases, the MX10008 devices did not support these DDoS protocol statements.

  - `Filter-action`
  - `Virtual-chassis`
  - `Ttl`
  - `Redirect`
  - `Re-services`
  - `Re-services-v6`
  - `Rejectv6`
  - `L2pt`
  - `Syslog`
  - `Vxlan`

  [See protocols (DDoS)].

- **sFlow configuration**—sFlow configuration is allowed only on -et, -xe, and -ge interfaces in EVO-based platforms. All other interfaces are blocked for configuring sFlow on EVO platforms. A cli error will be thrown if sFlow is configured on any other interface other than et, xe or ge interface.

- **New ARP and NDP packet classification**—We've introduced two CP classes for ARP and NDP packets received over VTEP interface. When your device identifies a packet as ARP or NDP, it performs an ingress port check which verifies whether the VTEP interface receives these packets. If VTEP interface receives the packet, datapath re-writes the CP class to the newly defined values. Based on this new CP class, the system performs the remaining packet processing and forwards the packets toward the host path. The system adds a separate DDoS policer to this ARP traffic, which ensures that the ARP traffic is not triggering underlay ARP DDoS violation.

MPLS

- **Display flexible algorithm information for SRv6 locators in TED database**—Use the `show ted database extensive` command to view the metric, flags, and flexible algorithm information associated with a SRv6 locator. In earlier releases, this information was not included in the TED database.

  [See show ted database].

- **CSPF LSP resignaling uses new instance ID (MX480)**—A Constrained Shortest Path First (CSPF) LSP uses a new instance ID when attempting to resignal an LSP that is down. In earlier releases, the CSPF LSPs that went down were stuck in CSPF path computation stage. You had to manually clear the affected LSPs and recompute the paths for the LSPs to be up again.

  [See LSP Computation.]

Platform and Infrastructure

- **Enhanced bandwidth and burst policer value**—We've updated the default bandwidth value from 20000 to 100 pps and burst policer value from 20000 to 100 packets. This enhancement avoids the CPU usage of `eventd` and `snmpd` reaching more than 100 percent. Earlier to this release, when the system receives a violated traffic for SNMP along with other protocols traffic, the CPU usage of `eventd` and `snmpd` was reaching more than 100% with an error.

  [See show ddos-protection protocols parameters.].

Subscriber Management and Services

- **Modified `show ancp subscriber details` output fields (MX Series)**—As the access loop encapsulation is transport independent it can be either passive optical network (PON) or DSL TLV. Hence, the `show ancp subscriber details` output field should not tag the details as a DSL TLV. Therefore, we've modified the existing `DSL Line Data Link`, `DSL Line Encapsulation`, and `DSL Line Encapsulation Payload` output fields to the following respectively:

  - `Access Loop Encapsulation Data Link`
  - `Access Loop Encapsulation Encapsulation1`
  - `Access Loop Encapsulation Encapsulation2`

  [See show ancp subscriber].

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

- In a scaled setup with LDP over RSVP configuration and maximum-ecmp as 32 or 64, line card CPU usage can remain high for extended duration on link flap operation. In this duration, LACP might take more than 5 minutes to converge and the aggregated Ethernet bundle to be active. PR1624219
- If proper gap is given between channelisation and dechannelisation the issue is not seen. Proper gap means allowing the system to complete the previous configuration before we load the new configuration. Recommendation is to if we give channelisation configuration commit wait for the links to come up or atleast the physical interfaces get created on both EVO and Junos OS Routing Engine and then only revert the configuration to dechannlisation and vice versa.PR1665625
- For GNMI subscriptions, Packet Forwarding Engine doesn't support filtering in subscription paths. So data is streamed from Packet Forwarding Engine ignoring filtering. PR1668911

Infrastructure

- When upgrading from pre 21.2 to 21.2 and onward, validation and upgrade will fail. The upgrading requires using of 'no-validate' knob. PR1568757
- Below IPC timeouts logs can be seen for statistics query to kernel(queried from cli or daemons querying internally)when there is config churn, or large number of IPCs getting exchanged between kernel and pfe in the system. if_pfe_msg_handler: pfe_peer_msg_handler error: error for msg type type, msg subtype subtype, opcode op and peer index index Default IPC timeout value in kernel for IPC statistics request is 10s. This can be incremented to larger value by setting below hidden config to avoid IPC timeout errors. # set system stats-timeout-lifetime 15 # commitPR1629930

Platform and Infrastructure

- In some scenarios with MPC, major alarm and following messages are generated. This major error is triggered due to parity error, and the impacted queue might drop packets. This might impact the forwarding, to recover MPC card need to be rebooted. PR1303489
- On MX and EX9200 serial platforms, under Ethernet VPN (EVPN) environment, packets routed using IRB interface could not be fragmented due to media maximum transmission unit (MTU) problem. PR1522896
- After a switchover event, when ppmd calls sendmsg system call to transmit the protocol packets, it gets blocked long enough that a few sendmsg calls cumulatively take up around 7 to 8 seconds. This

indirectly impacts the BFD session because the BFD session has a Routing Engine-based detect time of 7.5 seconds to expire. PR1600684

Segment Routing

- You can use IPv6 loopback address only as remote host address and cannot use as transit address in the segment ID (SID) list.
- An SID stack on ingress supports upto 6 SIDs.
- The `srv6 spring-te sids-stack ping` and `traceroute` commands are supported only in operational mode.
- You cannot enter duplicate SIDs for `srv6 spring-te sids-stack ping` and `traceroute` commands.
- SRv6 traceroute supports base ISIS instance.

Services Applications

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

VPNs

- In some scenario(e.g configuring firewall filter) sometimes srx5K might show obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. PR1432925

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

- In PBB-EVPN (Provider Backbone Bridging - Ethernet VPN) environment, ARP suppression feature which is not supported by PBB might be enabled unexpectedly. This could cause MAC addresses of remote CEs not to be learned and hence traffic loss. PR1529940

Forwarding and Sampling

- When the "fast-lookup-filter" statement is configured with a match that is not supported in the FLT hardware, traffic might be lost. PR1573350

General Routing

- If a vmhost snapshot is taken on an alternate disk and there is no further vmhost software image upgrade, the expectation is that if the current vmhost image gets corrupted, the system boots with the alternate disk so the user can recover the primary disk to restore the state. However, the host root file system and the node boots with the previous vmhost software instead of the alternate disk. PR1281554
- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. PR1362609
- FPC crash on MX240 and MX2020 routers or Packet Forwarding Engine crash on MX104 routers might happen when the MIC-3D-8OC3-2OC12-ATM is installed and ATM interface is configured. PR1453893
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- On all Junos OS platforms, after performing back-to-back rpd restarts, rpd might crash. The rpd core may be observed after a timeout of 10 minutes. PR1472643
- When there are HW link errors occurred on all 32 links on an FPC 11. Because of these link errors, all FPCs reported destination errors towards FPC 11 and FPC 11 was taken offline with reason "offlined due to unreachable destinations". PR1483529
- After backup Routing Engine halt, CB1 goes offline and comes back online; this leads to the backup Routing Engine booting up, and it shows the reboot reason as "0x1:power cycle/failure." This issue is only for the RE reboot reason, and there is no other functional impact of this. PR1497592
- In MAC-OS platforms when Juniper Secure Connect client connects successfully, the client is not getting minimized to tray icon and needs to be minimized manually.PR1525889
- Due to BRCM KBP issue route lookup might fail. PR1533513
- In scaled MX2020 router, with vrf localisation enabled, 4 million nexthop scale, 800K route scale. FPCs may go offline on GRES. Post GRES, router continues to report many fabric related CM_ALARMs. FPC may continue to reboot and not come online. Rebooting master and backup Routing Engine will help recover and get router back into stable state. PR1539305
- High CPU utilization observed for RPD after applying test configuration. PR1555159
- 5M DAC connected between QFX10002-60C and MX2010 does not link up. But with 1M and 3M DAC this interop works as expected. Also, it is to be noted that QFX10002-60C and ACX or traffic generator the same 5M DAC works seamlessly. There seems to be certain SI or link level configuration on both QFX10002-60C and MX2010 which needs to be debugged with the help from hardware and SI teams and resolved. PR1555955

- With IPsec PMI/fat-core file is generated, when `show services sessions utilization` CLI does not display the CPU utilization appropriately. PR1557751
- The Sync-E to PTP transient simulated by Calnex Paragon Test equipment is not real network scenario. In real network deployment model typically there will be two Sync-E sources (primary and econdary) and switchover happens from one source to another source. MPCE7 would pass real network SyncE switchover and associated transient mask. PR1557999
- VE CE mesh groups are default mesh groups created for a given routing instance. On VLAN or bridge-domain add, flood tokens and routes are created for both VE and CE mesh-group/flood-group. Ideally, VE mesh-group doesn't require on a CE router where IGMP is enabled on CE interfaces. MX Series linecard based CE boxes have unlimited capacity of tokens, so this would not be a major issue. PR1560588
- This is a feature enhancement and work is in progress to provide this support. This will have impact only when routing daemon crashes and will not have impact on rest of the NSR support. PR1561059
- Due to a race condition, the 'show multicast route extensive instance instance-name" output can display the session status as Invalid. Such an output is a cosmetic defect and not indicative of a functional issue. PR1562387
- To avoid the additional interface flap , interface hold time needs to be configured . PR1562857
- This issue is caused by /8 pool with block size as 1, when the config is committed the block creation utilizes more memory causing NAT pool memory shortage which is currently being notified to customer with syslog tagged RT_NAT_POOL_MEMORY_SHORTAGE. PR1579627
- In rare circumstances when doing routing-engine switchover, the routing protocol daemon in former active routing-engine (new backup routing-engine) might restart with a coredump while in process of being terminated.PR1589432
- On all devices running Junos 19.1R3-S5-J3, the subscriber IFL(logical interface) may be in a stuck state after the ESSM (Extensible Subscriber Services Manager) deletion. PR1591603
- This crash might be seen intermittently When config for interface associated with service set is changed, during handling of this config change crash happens due to incorrect pointer typecasting.PR1596578
- Pim Vxlan not working on TD3 chipsets enabling VxLAN flexflow after release 21.3R1. Customers Pim Vxlan or data plane VxLAN can use the version 21.3R1. PR1597276
- MX2010, MX2020: MPC11E: ISSU is not supported for software upgrades from 21.2 to 21.3 and 21.4 releases due to a flag day change PR1597728
- During RE switchover, if there is a burst of ICMP/BFD/SSH/FTP/TELNET/RSVP packets (~18K pps) you might see new backup RE restarting. PR1604299

- Correct the partition size so vmcore can be generated, when needed.PR1604755
- On MX-VC (Virtual Chassis) platforms with MS-MPC or SPC3 service cards and AMS(Aggregated Multi-Service), traffic on the line card in the backup chassis may not be load-balanced properly due to timing conditions. This works well on the line card in the master chassis. There might be traffic loss when interfaces are not properly balanced.PR1605284
- On all MX platforms, in a subscriber management environment, new subscribers might not connect if CoS (Class of service) CR-features (Classifier Rewrite) are used by the VBF (Variable Based Flow) service. The reference count mismatching between RE (Routing Engine) and VBF is caused by VBF flow VAR CHANGE failure. PR1607056
- Several warning messages show up while the RPD process restarts during performing GRES on a system running Junos EVO. PR1612487
- In some NAPT44 and NAT64 scenarios, Duplicate SESSION_CLOSE Syslog will be seen. PR1614358
- For ACX5448, MX204 and MX2008 "VM Host-based" platforms, starting with Junos 21.4R1 or later, ssh and root login is required for copying line card image (chspmb.elf for MX2008) from Junos VM to Linux host during installation. The ssh and root login are required during installation. Use "deny-password" instead of "deny" as default root-login option under ssh config to allow internal trusted communication. Ref https://kb.juniper.net/TSB18224 PR1629943
- On MX platform with enhanced subscriber management enabled, when "host-prefix-only" is configured on the underlying-interface for subscribers, it might not work in FPC. PR1631646
- The fabric statistics counters are not displayed in the output of "show snmp mib walk ascii jnxFabricMib". PR1634372
- On all devices running Junos OS or Junos OS Evolved, where this is a high BGP scale with flapping route and the BGP Monitoring Protocol (BMP) collector/station is very slow, the rpd process might crash due to memory pressure.PR1635143
- WIth PTPoIPv6 on MPC2E 3D EQ, PTP slave stays in acquiring state.PR1642890
- When CFP2-DCO is used, operator need to configure otn-option - that is the only mode supported PR1643815
- On MX10004/10008/10016 platforms, oamd process is not started and GRE keepalives adjacency is down.PR1644480
- Committing config changes during the PFE reset pause window (when PFE is disabled, yet the PFE reset proper has not started yet) has the potential of causing errors and traffic loss. In particular, config changes that result in re-allocating policers (which are HMC-based) might lead to traffic being entirely policed out (i.e. not flowing). Once the PFE reset procedure has started config changes ought to be avoided until the procedure is completely done.PR1644661

- On Daniel linecard, for PTP to work, port speed should be configured under the PIC heirarchy for both the PICs. (pic 0 and pic1) 1) When port speeds for some additional random ports are configured under the PIC hierarchy when PTP is configured, in that case PTP may fail. 2) When we perform PIC deactivate/activate, PTP gets stuck in acquiring state. 3) When port speed is not configured under PIC heirarchy, PTP will fail to go to Phase Aligned state. 4) Even with port speed config, PTP may still fail randomly. PR1645562

- With overlapping NAT pool configured with different NAT rules under different service sets, when service outside interface is moved between different routing instances (EX: from vr1 to default, and from default to vr1), NAT routes corresponding to the service-set in default routing instance are getting deleted, resulting in reverse path traffic failure for NAT sessions. PR1646822

- In the IPv6 segment routing deployment, packets are sent out with the wrong ethernet type. PR1647622

- V6 default route will not get added after successful dhcpv6 client binding on PTX1000 router during ztp PR1649576

- This issue occurs when the interface flaps (goes down and comes up within 1 second hold-off time), And if this happens twice in a sequence, we get into holdover issue. This issue is not specific to Daniel line-card, this can be seen in Indus line-card too.PR1654008

- Core dump reported intermittently where random grpc stack crash is observed. The license service will auto restart and recover.PR1656975

- Interop for 1G interfaces between EX4100 SKUs and acx5448/acx5448-M/D or MX480 will not workPR1657766

- During startup of a cBNG container or when JSD is restarted from the CLI in a cBNG container, JSD might crash creating a core dump. JSD should recover from the crash and automatically restart. JSD should function normally after recovering from the crash.PR1659175

- For MX204, MX10003, ACX5448 platform, if a non-default ssh port is configured for system login, after upgrade to 21.4 release, the FPC is stuck in offline. To avoid such issue please use default SSH port and use protect RE filter to only allow the access from the trusted source.PR1660446

- EX4600 and QFX5100-24Q devices VC (Virtual-chassis) is in unstable state for 3-7 minutes causing traffic loss.PR1661349

- On EX92XX series and MX platforms with the EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) scenario, the DHCP (Dynamic Host Configuration Protocol) packets from the client get dropped while tunneling to the EVPN-VXLAN. When this happens, the packets will not reach the DHCP server and the host could not get the IP address.PR1662524

- The version details for certain daemons will appear in the command output after the device has been rebooted after the completion of the USB installation of Junos.PR1662691

- The command "show chassis fpc" shows inaccurate information about heap memory in output.PR1664448
- Avoid change of user mesh group (HVPLS) instead delete or add. PR1667310
- user should not modify the locator attributes, instead locator, SIDs should be deleted and configured back. Otherwise it will lead to coredump.PR1667320
- On EX4100 platforms, delay in the CLI display for PoE commands might be observed when more POE devices with LLDP enabled (Power via MDI) are connected to the switch in a scaled environment with Perpetual POE scenarios. The LLDP PD requested power for all the ports are processed for each of the connected PDs, however the values in CLI display (CLI sync) might be delayed. PR1671311
- In over temperature situation, there will be a 10s timer before device bring the FPC down . However in some situation due to high temperature, a FPC offline action will be triggered before the 10s timer expires. Then the FPC will stuck in Present/Announce offline state. Cli offline/online it or physical reseat will not be able to recover the issue. When the issue happening, you may observe log message " graceful offline in progress, returning false" flooding: (date) (time) fpc_ok_to_start_generic: [FPC 0] gracefull offline in progress, returning false (date) (time) fpc_ok_to_start_generic: [FPC 0] gracefull offline in progress, returning false. Below MPCs are affected by this issue: MPC7/8/9 MPC10 MPC11 LC480 LC2101 LC9600 LC304 LC4800 FPC-P2, FPC-P3. PR1676008

High Availability (HA) and Resiliency

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

Interfaces and Chassis

- Error logs related to invalid anchor next hops are seen when the MPC10 or MPC11 FPCs are restarted with distributed aEthernet IRB VRRP sessions. The aggregated Ethernet should span multiple FPCs.PR1674069

Layer 2 Features

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

MPLS

- In MVPN Case, if the nexthop index of a group is not same between master and backup after a nsr switchover, we may see a packet loss of 250 to 400 ms. PR1561287
- Ingress will retry after LSP stay down for extended period of time or customer can clear lsp to speed up the retry. PR1631774

Network Management and Monitoring

- When `maximum-password-length` is configured and user tries to configure password whose length exceeds configured maximum-password-length, error is thrown, along with error 'ok' tag is also emitted. (Ideally 'ok' tag should not be emitted in an error scenario.) The configuration does not get committed. PR1585855
- The mgd process might crash when an invalid value is configured for identityref type leafs/leaf-lists while configuring Openconfig or any other third-party YANG, problem happens with json and xml loads. PR1615773

Platform and Infrastructure

- On all Junos and Junos OS Evolved platforms, while using source-address NTP configuration parameter and issue the command "set ntp date" from the CLI, packets will be sent with the source address of the outgoing interface rather than the manually configured IP address. Typically, the manually configured IP address would be a loopback address. The problem does not apply to automatically generated NTP poll packets.PR1545022
- When the `deactivate services rpm` and `deactivate routing-options rpm-tracking` configuration statements are committed, some of the rpm tracked added routes are not deleted from the routing table. As a workaround, deactivate routing-options rpm-tracking, commit the configuration. As a result, all the

rpm tracked routes are deleted. To deactivate the RPM service, deactivate services rpm and commit. PR1597190

- With given multi dimensional scale, if configuration is removed and restored continuously for more than 24 times, MX Series based FPC might crash and restart. During the reboot, there can be traffic impact if backup paths are not configured. PR1636758

Routing Protocols

- On all platforms, the issue is when the first time when ESIS is coming up sometimes the ESIS route might not get installed. PR1559005
- Any platforms with micro BFD configured on member links of the LAG/ae interface, BFD Session state in Routing Engine remains as UP always even though PEER device has ceased.PR1675921

Routing Options

- When an AMS physical interface is configured for the first time or any member of the AMS bundle is removed or added, the PICs on which the members of AMS bundle are present reboots. There is a timer running in the AMS kernel which is used as a delay for the PIC reboot to complete. After the timer expires, AMS assumes that the PICs might have been rebooted and it moves into next step of AMS fsm. In scaled scenarios, this rebooting of the PIC is delayed due to DCD. This is because when a PIC goes down, DCD is supposed to delete the physical interfaces on that PIC and then the PIC reboots. But DCD is busy processing the scaled configuration that delays to deleter the physical interface. This delay is much greater than the timer running in AMS kernel. When the above timer expires, the FSM in AMS kernel incorrectly assumes to complete the PIC reboot. But the reboot is still pending. By the time DCD deletes this physical interface, the AMS bundles are already UP. Because of this, there is a momentary flap of the bundles. PR1521929

Services Applications

- L2TP LAC functionality is not working in this release when MX Series router are operating and a BNG-UP. PR1642991

VPNs

- Change here is basically reverting to old enum value used for ATM VPN, and using a new value for BGP multicast address family, and although these are not visible behavior change, due to this, there may be impact on unified ISSU for ATM VPN and BGP multicast address family if enabled.PR1590331

Resolved Issues

IN THIS SECTION

EVPN

- The rpd process crash might be seen due to memory allocation failure. PR1636690
- The DF and BDF both might be up or forwarding in EVPN multihoming single-active scenarios. PR1647734
- The spine might have stale VTEP entry for the ESI even though the host MAC is not advertised by the leaf. PR1648368
- ARP/NS response to anycast IRB might fail due to missing mac-ip entry. PR1650202
- EVPN VXLAN type 5 does not work with asymmetric VNI configuration. PR1652339
- The rpd process might crash when EVPN protocol is deactivated. PR1659786

Forwarding and Sampling

- mib2d core hitting @mib2d_fwstats_async_handler_cb rtslib_async_process_msg during GRES testing with page pooling enabled. PR1647669
- The MPC or FPC crash is seen on specific LC's running BGP flowspec. PR1662955
- Traffic loss is observed in the VPLS scenario after the upgrade. PR1663717

General Routing

- FPC generaltes a core file if CFM flap trap monitor feature in use. PR1536417
- SESSION CLOSE Termination reason is "other" (very generic reason) when the server initiated sessions are closed due to PCP life time expiry. PR1588785
- The Routing Engine goes into a fault state if `request node power-on` CLI is executed while the node is powering off. PR1589737
- DHCP offer packets received on MPLS enabled interface might be dropped by the BNG working as a relay agent in a subscriber management enabled environment. PR1608592
- `show ldp traffic-statistics interface p2mp` do not display any traffic statistcs. PR1611498
- A device which is configured IP interface (ip-x/x/x) cannot sent out encapsulated IPv4-over-IPv6 packets to a remote device in case of transit packets. PR1618391

- Traffic might dropp due to the TX queue memory leak on PCI interface. PR1618913
- /interfaces/interface/subinterfaces/subinterface/state/counters not exported during initial synchronization for on-change. PR1620160
- You can observe the cosd core file after Routing Engine switchover. PR1620758
- BFD session flaps in scaled scenario. PR1621976
- chassis alarm "VMHost RE 0 Secure BIOS version mismatch". PR1622087
- BGP flowspec might not show counters. PR1623170
- We observe flowd core file with TLB configuration only with combination of MPC10 card with older MPC card. PR1624572
- Pkid crashes due to null pointer dereferencing during local certificate verification in some cases.PR1624844
- Fabric request timeouts and fabric healing occur. PR1625820
- Subscribers might face connectivity issues due to memory leak. PR1627562
- Interface sensor data might not be decoded on line cards (MPC10E/MPC11/MPC12/LC9600) and Junos Evolved platforms. PR1628807
- FPC might crash in the subscriber scenarios. PR1629136
- LC9600 might go to an offline state due to the chassis connection drop after fresh USB installation. PR1629558
- You might observe Config-Sync failure alarm. PR1629952
- Fabric drops with SCBE3+SPC3 around 10M PPS/60G TCP traffic with approximately 750 byte packet size with IPv6 SFW on a single PIC. PR1630223
- Late drops are not at par with PN configured. PR1630724
- On MX Series platform interface stays down till the hold-up timer is expired during a Packet Forwarding Engine reset. PR1630793
- Multicast traffic received from an external source may not be sent to the multihomed listener interfaces PR1631249
- A clksync might crash and PTP might get stuck. PR1631261
- Precision Time Protocol (PTP) might not lock on MX Series with MX-MPC2E-3D-P and MPC2E-3D LC. PR1631274

- [macsec] [fips MPC7E] FPC/PIC must reboot on fake KATs generation. PR1632273
- DSLite might not work on MX Series devices with MPC7E line card and SPC3 service PIC. PR1632278
- Single hop BFD session over aggregated Ethernet stuck at INIT after "reset PFE". PR1632585
- "show chassis firmware" does not show the revision for PIC FPGA. PR1633187
- In subscriber scenario, traffic drop might be seen when you remove aggregated Ethernet member link. PR1634371
- LACP interface might go down when a sub-interface configuration is added and committed to the aggregated Ethernet interface. PR1634908
- Post Packet Forwarding Engine reset error information is not going out from "show system errors active detail". PR1635284
- IPv6 route advertisement sent on management interfaces might cause other devices to fail to get the dhcpv6 address. PR1635867
- IPsec tunnel might not establish after a flap. PR1635882
- After the core interface flap, some IPsec sessions fails to come up. PR1636164
- Same VLAN cannot be used as data VLAN and voip VLAN together. PR1637195
- FPC crash might be seen on all MX Series platforms with BBE subscriber. PR1637304
- Syslog error @Err] MQSS(0): DRD: Error: WAN reorder ID timeout error - Valid 1, Reorder ID 0 after loading image. PR1637756
- MACsec traffic drops when you perform back-to-back graceful switchover. PR1637822
- Packet Forwarding Engine might get stuck after 100G/400G interface flap. PR1638410
- Kernel might panic while rebooting. PR1638923
- USB device is not visible in Junos OS. PR1639071
- The dynamic tunnel might flap every 15 minutes with a non-forwarding route. PR1639134
- LC9600 having less required planes for fabric bandwidth degradation behaviour. PR1639212
- High CPU utilization for rpd might be seen. PR1639252
- When you issue panic command, dump is complete. While rebooting, the box is stuck. PR1639459
- KRT queue entries are stuck during Routing Engine switchover when backup RPD is not yet ready. PR1641297

- Out of order packets might be seen in multicast streams with MVPN extranet scenario. PR1641323
- The mesh group configuration does not get activated after configuring the mesh group under the deactivated routing-instance and then activating. PR1641412
- Traffic might be dropped due to the RX queue being full. PR1641793
- MPC10E: Quick 100G link-flaps has still some race conditions which can cause MQSS stream drain failures and xqss_sched_flush_queue failures. PR1642584
- CRC/ALign errors reported on dual marvell ports when pic is bounced in 25G mode with number of ports configuration changes. PR1643433
- Communication loss between master Routing Engine and backup Routing Engine with temperature-threshold configured for MPC3E-NG. PR1643739
- RIP NSR state might be stuck in InProgress after Routing-Engine switchover. PR1644274
- The openconfig network-instance/protocols/static-routes/static id list-key might generate an error on encoding through NETCONF. PR1644319
- The oamd process might not start and GRE keepalives adjacency is down. PR1644480
- Stateful synchronization fails between active and backup MX Series chassis. PR1644579
- Traffic drop with EBGP multipath and EBGP paths equal to the maximum-ecmp limit. PR1645296
- The interfaces might remain down and loopback wedge error might occur. PR1645431
- The rpd crash might occur in backup Routing Engine. PR1645457
- DHCP dual stack subscriber scale-up failed in access model DHCP relay. PR1645574
- The eBGP session might not be established on MX Series platforms with MS-MPC and MX-SPC3 cards. PR1645585
- The Routing Engine mastership might not transfer on each rpd crash. PR1645611
- Pseudo devices connect on ud and ut interfaces that stay down after host FPC restarts PR1645671
- The alarm might not be generated for EDAC errors until the FPC reboots. PR1646339
- Error messages "LOG: Err] stats_lu_counter_read_internal(1430): pfe 0:[NH Cntr] jnh[0x1] != cnh" seen after loading configurations. PR1646401
- While updating ca-profile-group certificates, all Junos OS and Junos OS Evolved platforms might face certificate load failure when a configuration commit is made in the background. PR1646925

- The 'show ancp subscriber details' CLI output for Access Loop Encapsulation tlv is updated. PR1647180
- DHCP subscriber traffic might drop due to the rpf-check filter. PR1647214
- Changing error severity is not working on FRUs managed by Routing Engine. PR1647282
- Services might not work with the "VLAN-rewrite" configuration. PR1647294
- Traffic drops after switching of VNIs across two VRFs in EVPN/VXLAN scenario. PR1647516
- [MULTICAST]upstream rpf session status in not expected state stuck in Init state. PR1647746
- "set vmhost management-if add-policer" configuration not taking effect. PR1647750
- When PTP with PHY-timestamping is enabled, significant clock frequency drift might be seen PR1647901
- chassis-control subsystem went to unresponsive state after FHP phase2 trigger PR1648030
- Interoperability issue between TRIO line cards and MPC10E and MPC11E AFT cards cause incorrect egress load balancing over Aggregated Ethernet links PR1648059
- High inter-packet delay and throughput performance degrade for PFE sensors PR1648133
- Modifying NH that as indirect nh addr to setting decapsulate_header does not work PR1648162
- The mspmand process crashes on MX router with MS-MPC card PR1648428
- While sending BGP NOTIFICATION messages for RFC 8538 HARD RESET, the data portion is sometimes not present PR1648479
- MX960 :: bbe-statsd core observed at vlogging,smid_reregister, sdb_db_check,Juniper: :SmidInterface:: isReady in bbe-smgd daemon restart test PR1648565
- MPC10/11 line cards may crash PR1648750
- EVO snmpwalk do not return value for index 0 PR1648760
- Subscriber load-balancing not supported in release PR1649062
- Firewall counters might not increment for a longer time PR1649324
- PTX10008 EVO SyncE clock 'hold-off-time' configuration not working due to incorrectly computed timer value PR1649358
- The MPC might crash or the traffic may be silently dropped/discarded PR1649499
- BGP Sensor "/bgp-rib/afi-safis/afi-safi/ipv4-unicast/loc-rib/" not available as a 'periodic' sensor PR1649529

- Junos OS: PTX Series: FPCs may restart unexpectedly upon receipt of specific MPLS packets with certain multi-unit interface configurations (CVE-2022-22202) PR1649586
- Auto detection of affected YT from ZF parity error. PR1649858
- [subscriber_services/5g-pfcp] [show] mx480 : :: Test-11_3 (RLI-49857) fails in CATS. ~5000 sessions in wait state during login after apfe failover. PR1649861
- MPC11 interface might remain down after flaps. PR1650178
- IRP memory parity issue might result in traffic loss on PTX and QFX10k Junos platforms PR1650217
- Traffic Loss will be observed with Virtual-Router PR1650335
- The IPv4 traffic drop might be observed in EVPN scenario PR1650854
- VMcore is triggered when control packets go over IRB and GRE PR1651273
- The BFD session might flap in some scaled system with churn PR1651473
- Chassis alarm "Major CB 0 external-1/0 LOS" can be seen after upgrading to 21.2R3 PR1651490
- PCS Errored blocks count will increment after Junos software upgrade to 20.2R1 or above releases PR1651526
- EX9251 :: Reboot reason shows as "0x2000:hypervisor reboot" instead of "0x4000:VJUNOS reboot" when we do Junos reboot PR1651721
- An error might be seen when the member link on an AE bundle is deleted PR1651932
- Subscribers cannot bind on a BNG-UP after the access interface has been disabled and re-enabled. PR1652203
- The L2BSA subscribers might not be able to browse due to incorrect entries in the VPLS mac-table. PR1652337
- An rpd core file might be seen with back-to-back rpd restarts. PR1652387
- P2MP traffic loss might be seen when link protected LSP revert back to the primary path PR1652651
- The syslog errors and PPE traps might be observed PR1652901
- The rpd might crash when BMP rib-out monitoring is configured for flow-spec route PR1653130
- Additional debug logs may be printed onto device console, when device is booted from a bootable USB PR1653499
- BGP PIC Edge might cause traffic Black-holing after selector corruption PR1653562

- Due to the MAC learning limit being exceeded traffic drop might be observed in the MC-AE scenario PR1653926
- When fib-streaming is enabled and two or more collectors are involved, fibtd core may be observed due to a timing sync issue PR1653942
- The ARP might not resolve with the native-vlan configuration PR1654215
- LACP sent IN SYNC to server facing interface when core-isolation is in effect. PR1654459
- In a subscriber scenario, AAA module of "mobiled" process may cause memory leak on the standby routing-engine PR1654947
- EVPN-VXLAN: ex4100 :PDT:: Partial traffic drop seen on the emerald VC , after RE switchover from primary to back up with NSR/NSB. PR1655052
- BFD may flap when the hold down/up timer is configured PR1655088
- The 1G port always stays down while changing of 10G interface lane speed to 1G PR1655089
- The 400G ports might not come up on MX platforms PR1655459
- [gRIBI]IPIP tunnel remains in the PFE even after clearing all programmed route entries PR1655531
- UEFI BIOS Key synchronization tool - efitools.service failed after optics diagnostics test. PR1655537
- Certificate-based VPN tunnel is not established. PR1655571
- pkid core seen and can see interfaces lost PR1655949
- The Configuration of invalid forwarding-class in analytics export profile goes through may lead to traffic drop PR1656313
- GRE-in-GRE encapsulated traffic might be dropped when the recursion-control bit is set to non-zero, which does not comply with RFC standard PR1656499
- Decapsulation and look up in default instance will not work if backup next-hop groups are added after adding the routes PR1656561
- jnxDomCurrentLaneRxLaserPower SNMP MIB is not providing lane 0 information if polled using ifindex without Lane number PR1656702
- The configuration of management interface might not work PR1656746
- 22.2R1:: MISC:: mspmand core found @sarena_free @mum_free @jsf_shm_free @jssl_mem_pool_free @jsf_openssl_free @CRYPTO_free @ssl_cert_free @jssl_config_dtor @msvcs_plugin_send_control_rt PR1657027
- The transit traffic might be impacted in the PTP scenario PR1657132

- SR-TE LSP state might go down due to "Compute Result failure" PR1657176
- Delete AFT Operation for PolicyForwrdingEntry is not deleting policy filter for single SINGLE_PRIMARY mode PR1657208
- The low priority stream may get stuck and all traffic might be dropped PR1657378
- AE bundles with member links from MPC10 does not have VLAN-REWRITE feature programmed correctly PR1657465
- The rpd might fail on backup RE on EVO platforms PR1657797
- The validation fails if a media install Junos upgrade is performed PR1657840
- The 'agentd' and 'eventd' process might cause high CPU utilization and may also affect Telemetry services PR1657886
- jsd deadlock when grpc connections are in closed state PR1657943
- AFT sensor UDP output not decodable using Junos Proto file. PR1658017
- The jdhcpd process might be stuck at 99% if traceoptions is enabled in high DHCP traffic scenario PR1658087
- TOS(DSCP+ECN) bits not getting copied from the Inner L3 header to Outer VXLAN header. PR1658142
- "request system scripts refresh-from op.. " output is not working as expected PR1658154
- Fabric Destination error/Fabric plane in check state PR1658164
- The CPU usage SPMB can hit 100% for a short while PR1658206
- Some L3VPN prefixes are not active because nexthop is not usable PR1658277
- The rpd crash might be triggered when the BGP route resolves over another BGP route PR1658678
- Valid software licenses might not be in sync between members in the Virtual chassis. PR1658913
- The rpd memory leak might be seen while processing vlan-ccc configuration PR1659102
- The multipath route might be missing when multipath is configured PR1659255
- Multiple stale EIM mappings observed on Junos MX platforms due to the aging timer getting stuck PR1659284
- State gRIBI clients not cleaned up PR1659442
- Traffic loss might be seen when a VxLAN port is recovering from a failure PR1659533

- The configuration might roll back after performing "commit confirmed" and then reboot PR1659783
- After changing the MTU on an aggregated interface along with IRB the kernel crash might be observed PR1660208
- Soft assertions in RPD will fail during GRES PR1660484
- Transit PTP over IP packet drop might be observed on an AE interface PR1660844
- The evo-aftmand might crash when sFlow is enabled on FTI interface PR1661056
- Channelized interface might go down if low-light-alarm/low-light-warning is enabled PR1661215
- The l2circuit backup might not get reverted to primary in rare condition PR1661802
- The watchdog timeout is encountered and the system reboots after the 'request system halt' command executed PR1662913
- TCP MSS value might not get reflected to packets PR1662950
- network-instance name for streaming telemetry to be changed from default to DEFAULT to align with CONFIG stanza PR1662999
- The offset value might be high on the downstream node while switching between line cards which impacts 5G services PR1663065
- The forwarding plane is not updated properly in scaled MVPN scenario after receiving PIM leave messages PR1663568
- Subscribers will be stuck in the initializing or terminating state PR1663689
- Trinity-based line cards with VPLS and CFM configuration may crash when the indirect NH associated with LSI IFL is deleted PR1663725
- Syslog message related to SNMP tcp connection is seen from PCCD daemon post switchover in EVO PR1664165
- The routing process on the device might crash when the IP address of local interface is changed to the IP address of BGP peer PR1664527
- Line card may crash after offline/online plane PR1664602
- MAC addresses learned on the RTG interface are not aging out PR1664955
- The link-degrade recovery will not work for a specific interface speed PR1664978
- The rpf-check feature might not be working in a Junos Subscriber management scenario. PR1665234

- MAC-IP bindings for IPv4 (ARP) and IPv6 (ND) may not be processed for IRB interfaces in an EVPN scenario. PR1665828
- In the SRTE scenario, sensors are incorrectly populated for colored tunnel BSID routes when uncolored tunnels are enabled. PR1665943
- BGP-LU traffic might be dropped when "CCNH ingress labeled-bgp inet" is configured. PR1666760
- Traffic drop might occur on AF interface when Packet Forwarding Engine gets in disabled state on GNF in NodeSlice platforms. PR1666992
- The hyper-mode might be set incorrectly after power cycle on MX Series platforms PR1667226
- High numbers of PDs connected might result in high CPU utilization. PR1667564
- The FPC might fail to initialize on Junos OS platforms. PR1667674
- Shutting the CE interface and bringing back up causes traffic (going towards the core) drop PR1667724
- Periodic event generation doesn't work after Routing Engine reboots. PR1668152
- Timestamp uint_val isn't proper is streaming output. PR1668265
- The BGP multipath might not install some of the available next-hops. PR1668481
- EVPN PE router might respond traceroute with unexpected source IP address to remote CE device. PR1668837
- Commit configuration check-out failed while configuring syslog stream host IP in specific range. PR1668941
- Traffic loss might be seen for the multicast traffic. PR1668976
- The rpd process restarts after generating core file. PR1669346
- LLDP neighborship might fail if the chassis-id format of the LLDP packet is xx:xx:xx:XX:XX:xx. PR1669677
- Interoperability issue between legacy line cards and MPC10E/11E causes L2 packet drop. PR1669765
- MX150 platform reports error for bandwidth license. PR1671347
- The chassisd memory corrupts and the process crashes. PR1672039
- Traffic impact might be seen due to an unexpected reboot of SPC3 card. PR1672819

- Training failures reported on the MX2010/MX2020 Junos OS platforms post fabric plane offline-online. PR1673806
- During the smooth upgrade from SFB1 to SFB2, SFB2 gets detected as "Unknown Fabric Board". PR1674309
- The "nsd" may crash post NAT rule configuration change. PR1674381
- The 'kmd' process may crash due to SA re-negotiation failure during IKE phase-1 PR1674585
- Minor memory leak in 'bbe-statsd' daemon may be seen when subscriber-management is enabled on MX platforms PR1676049
- While processing SNMP GetNext requests 'trasportd' may reach 100% of CPU utilization PR1676593
- Fabric Plane check/error alarm would be seen due to the burst traffic in MS-MPC line cards PR1681624

Class of Service (CoS)

- The cosd process might not be able to send unbinds for rewrites post a certain sequence of operations are performed PR1649510
- Interface burst size becomes low in pfe, when 'rate-limit-burst' knob is removed PR1650089
- Hierarchical class of service (HCOS) might not work for LT interfaces configured on PIC 2 and PIC 3 of MPC5E/MPC6E PR1651182
- The rewrite rule might not work configured on L2 VLAN CCC IFL PR1655371
- COS SMAP config not getting applied on AE IFLs PR1656441
- QoS may not work as expected on AE interfaces with explicit-null label PR1675781

General Routing

- The rpd-agent process might crash with a high scale of member nexthops PR1640224
- The jdhcpd daemon might crash after Junos upgrade PR1649638
- The rpd agent crash might be triggered after the interface flap for the backup RE PR1652595

Interfaces and Chassis

- VRRP flaps between MC-LAG peers when deleting vlans on MC-AE interfaces PR1579016
- The FPCs might not come online after the USB upgrade method PR1637636
- Traffic loss might be seen for the mac addresses learned on the ICL interface PR1639713
- The lacpd may not come up on one of the links in the AE bundle PR1647145
- Authenitcation key can not be configured more than 15 character PR1650873
- VRRP failover over 2 seconds may be observed PR1652549
- [PTX10003] SSD DGM28-B56D81BCBQ || RE 0 SSD Primary minimum supported firmware version mismatch PR1654762
- 22.2TOT :SecPDT:Unified L4/L7 Use Case Sky ATP: reth1 interface down and DCD cores observed on node1 during test on 22.2TOT image PR1657021
- when moving few child members from one AE bundle to another AE bundle observed error log "UI_CONFIGURATION_ERROR: Process: dcd, path: none, statement: none, ae12, Micro BFD local address should be configured on ae12 or lo0" PR1658016
- Configuring a VIP from a different subnet (other than parent IP) might affect IPv6 VRRP sessions PR1658326
- The MAC address may be learned over the wrong interface in the MC-AE scenario PR1658742
- VRRP operations may flap when configuration changes are committed under unrelated VRRP groups present on the same physical interface PR1658966
- The VRRP track might go down upon GRES PR1668280

Juniper Extension Toolkit (JET)

- The connection might get closed by the collector when connecting to jsd PR1653968

Layer 2 Features

- The Pseudo Wires might go down in VPLS scenario PR1655858

Layer 2 Ethernet Services

- Traffic loss may happen when there is a mismatch of subscribers between the master and backup relay PR1638050
- DHCP packets might not be sent to the clients when 'forward-only' is reconfigured under the routing instance PR1651768
- JDHCPD core found @rcdb_v4_alq_packet_retry_queue_cleanup_tcp_conn after cleanup the pppoe sessions, dhcp and dhcpv6 server binding all PR1668015

MPLS

- An rpd core is seen post graceful switchover PR1635863
- The rpd process might crash when the P2MP Egress interface is deleted while LDP P2MP MBB is in progress PR1644952
- LSPs which are using the TED Database on JUNOS platforms running BGP-LS might not be able to compute paths properly PR1650724
- P2MP LSP flaps after the MVPN CE facing interface goes down PR1652439
- The route might stay up but LSP remains down after the primary LSP interface is administratively disabled PR1654226
- RE kernel crash might be observed in the one-hop-LSP MPLS scenario with RE outbound traffic if 'routing-option resolution preserve-nexthop-hierarchy' is configured globally PR1654798
- The "rpd" process may get crash when container Label Switch Path (LSP) is configured with "default-template" PR1655177
- Memory utilization keeps incrementing due to the path error message PR1657872
- LSPs are getting stuck in a down state after deactivating/activate protocol BGP PR1659340
- The LSP may get stuck in the CSPF path computation stage PR1661954
- Dynamic label space usage crossed the threshold limit of 90 percent PR1664670
- Transit LSR might stop sending RESV msg if there is no RRO in the LSP's PATH message PR1667708
- Premature RSVP Path Error BW-Unavailable originated by PLR PR1670638
- The rpd crash might be observed with Container LSPs PR1672804

- RPD cores very rarely when constructing LDP trace message irrespective of enable/disable LDP traceoptions PR1676503
- The traffic might drop when the Link State protocol with the least preference is set to active and fails the CSPF algorithm PR1677930
- In an LDP -> BGP LU stitching scenario, Multiple LSPs will not be installed in the forwarding table, even if BGP Multipath and ECMP are enabled PR1680574

Multicast

- Traffic blackhole might be seen due to next-hop install failure on Junos PTX platforms PR1653920

Network Management and Monitoring

- Observed memory leak in eventd leak during GRES PR1602536
- The module junos-configuration-metadata.yang is not downloadable via CLI/Netconf PR1643785
- Junos does not emit leaflist annotation in XML when client queries the XML as per RFC 7952 PR1647740
- VTEP might report a high speed on the sub-interface, causing SNMP alarms PR1651774
- The "snmpd" process might crash if SNMP timeout happens PR1666548
- The snmpd core might be observed with filter-duplicates configuration PR1669510
- While loading MIB file, saw error : "DESCRIPTION" is missing for "mib-jnx-chas-defines.txt" PR1670858

Platform and Infrastructure

- The core interface goes down PR1631217
- LMEM Parity Error in shared LMEM are not handled properly PR1652416
- Regressions : ifstraced.core-tarball.0.tgz found @ inet_ntop6>__inet_ntop>rtslib_ifsm_info_print>dump_all_ifstate_tracerec_from_kmem>ifstraced_go_trace PR1654737

- Multicast packet drop causes pixelization PR1655363
- Use `show firewall attachments` instead of `show firewall bind` for MX Series routers with MPC10 and above line cards to display the filter bind points through vty command. PR1655634
- PFE might get disabled if a packet with a small size is transmitted out of the queue. PR1657203
- The MPC crash might be observed for the IRB interface flap part of the layer 2 domain in a multicast scenario. PR1657983
- Lockout-period might not work as expected. PR1660931

Routing Policy and Firewall Filters

- Existing routing policies might change when global default route-filter walkup is changed. PR1646603
- The firewalld process might crash when nested filters are used as input list. PR1651411
- Old OC next-hop still shown in static route, discrepancy between OC stanza and Junos-yang. PR1662909
- The rpd process crashes whenever it is getting shut down with router reboot, rpd restart, Routing Engine switchover, software upgrade. PR1670998

Routing Protocols

- Initial multicast register packets might get dropped. PR1621358
- An IGMPv2 snooping proxy will originate IGMPv3 membership for a new group join request towards a multicast router. PR1637090
- The rpd crash files might be seen on MX Series and PTX Series platforms. PR1643089
- An error might be observed while executing a commit for openconfig instance type. PR1644421
- The rpd crashes on all Junos OS platforms. PR1648471
- RFC 8950 extended nexthop encoding capability conformance issue. PR1649332
- `show multicast snooping route extensive instance evpn-vxlan-A` with VLAN filter is not showing VE, AR mesh group route entries. PR1649410

- Delay in BGP session establishment due to longer time for the listening task to be ready on all platforms running "rpd". PR1651211
- Traffic loss might be seen when the new multicast composite next-hop is computed. PR1651824
- BGP PIC protection is not working in virtual router. PR1653356
- RPD core file might be generated while accessing logical interface of mpls-lsp-interfaces in ISIS (FA-LSP). PR1654162
- An RPD process crash might be observed, when the received prefix count exceeds the configured "prefix-limit". PR1655228
- The rpd process crash might be observed with PIM configured. PR1656311
- "--RT--" memory is slowly incrementing in `show task memory detail` output. PR1657321
- The memory leak and process rpd crash might be observed when the peer interface flaps continuously in the segment routing. PR1659366
- A policy with a policy action "community" configuration may not work. PR1660424
- Incorrect inactive routes are being propagated to neighbors with add-path. PR1660456
- The v4 prefixes might not be advertised over the BGPv6 sessions. PR1664168
- The BSR information might not be flooded over NG-MVPN. PR1664211
- BGP labeled-unicast inactive routes might not be advertised when add-path is configured. PR1665610
- The rpd crash is observed while making configurational changes. PR1669716
- BGP inactive routes may not be advertised to peers in BGP-LU scenario. PR1669930
- The rpd crashes upon receiving BGP multi-nexthops inetflow route in the 21.4 software release and onward. PR1670630
- The rpd can crash while route exchange using BGP and LDP in a rare scenario. PR1671081
- The backup next hop computation might not be as expected for some random prefixes when there is a topology change. PR1671672
- MCSNOOPD will be restarted and will again learn the states after core file is generated. PR1672488
- The IS-IS learnt routes might be downloaded to RIB again and again if the prefix attribute flags are different. PR1673953

- Inter-domain forwarding connectivity might be broken between different lo0s in the option-C network causing problems for MPLS transit-route. PR1677935
- Traffic drops due to the generation of the FPC core, which makes the system unstable. PR1678016
- RV task replication will be stuck in the "NotStarted" state when routing-options validation is deactivated/activated. PR1679495
- The rpd process will crash and generate core post graceful restart. PR1682778

Services Applications

- The kmd crash might be observed in IPsec scenario. PR1637906
- L2TP session might not come up when L2TP access-line-information is not configured. PR1667861
- VMcore or Routing Engine crash might be triggered due to the memory corruption when the FPC is restarted for LNS subscribers. PR1667950

Subscriber Access Management

- DHCP clients with static IP addresses binding might get disconnected. PR1650243
- Pool drain with APM do not work. PR1652715
- JDI-RCT:BBE:Authd core@thr_kill () at thr_kill.S:3. PR1655832
- New service profile provided by Radius during re-authentication triggered by DHCP Renew packet with changed actual data rate TLVs might not be applied. PR1665947
- CoA-NAK might not be sent for a coa-request-retry of the same service. PR1667002
- Errors are seen when the accounting server source address is IPv6. PR1669284

User Interface and Configuration

- Passwordless authentication successful for configured user even after deleting ssh public key details from user login hierarchy. PR1625032
- Configuration archive transfer does not happen via FTP. PR1625937

- Junos Fusion Satellite EX4300 upgrade fails from Aggregate Device MX104. PR1627323
- ISSU failure may be seen due to timer expiry. PR1634334
- MTU configuration on an interface is not set as expected. PR1636085
- TRACKING PR ::MX480 :: CORE-PR::bbe-smgd.core observered at 0x040e9caf in abort () at /.amd/svl-engdata5vs2/occamdev/build/freebsd/stable_12_213/20211023.042806__ci_fbsd_builder_stable_12_213.0.7016a19/src/lib/libc/stdlib/abort.c:67. PR1637272
- During the ephemeral configuration database changes, "mgd" core files might be generated. PR1637552
- Ignore the syslog - UI_MOTD_PROPAGATE_ERROR: Unable to propagate login announcement (motd) to /var/etc/motd.junos. PR1642743
- The ddos-protocol-group might not be listed in ddos-protection protocols violations display xml. PR1647046
- The traffic might not flow after deleting/adding VLAN configuration with load override. PR1647853
- The vlan-tagging configuration might cause the blank interface configurations after a system reboot or upgrade. PR1650151
- <!--

  JDI-RCT : QFX:5120 :MCLAG : l2ald core observed at ?0x0000000000676fed in l2ald_config_read_bridgedomain (insttype optimized out, obj=0x0, lr=0x0, rtt=0x3317010) at l2ald/l2ald_config_bd.c:2607 after loading test configurations. PR1652605

  -->
- Core file is generated during configured app restart test. PR1658688
- "gethostbyname: Host name lookup failure" is displayed during commit. PR1673176

VPNs

- The routing protocol process might stop working when de-activating and activating the same provider tunnel from one to another instance in a single commit. PR1647149
- MVPN Inter-AS option B shows updated PMSI attribute tunnel id when advertising type-3 routes to Intra-AS PE. PR1652481
- The device enabled with FIPS mode and rebooted the system fails to boot. PR1655355

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

The following table shows detailed information about which Junos OS can be used on which products:

Platform	FreeBSD 6.x-based Junos OS	FreeBSD 12.x-based Junos OS
MX5, MX10, MX40,MX80, MX104	YES	NO
MX240, MX480, MX960, MX2010, MX2020	NO	YES

Basic Procedure for Upgrading to Release 22.3R1

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 FreeBSD 12.x-Based Junos OS

Products impacted: MX240, MX480, MX960, MX2010, and MX2020.

To download and install FreeBSD 12.x-based Junos OS:

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

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

2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the Release drop-down list to the right of the Download Software page.
4. Select the Software tab.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
7. Review and accept the End User License Agreement.

8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new jinstall package on the routing platform.

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

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-22.3R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-22.3R1.9-signed.tgz
```

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-22.3R1.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-22.3R1.9-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***

Do not use the `validate` option while upgrading from Junos OS (FreeBSD 6.x, 10.x, and 11.x) to Junos OS (FreeBSD 12.x). This is because programs in the **junos-upgrade-x** package are built based on FreeBSD 12.x, and Junos OS (FreeBSD 6.x, 10.x, and 11.x) would not be able to run these programs. You must run the `no-validate` option. The `no-validate` statement disables the validation procedure and allows you to use an import policy instead.

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

Rebooting occurs only if the upgrade is successful.

NOTE:

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.
- Starting in Junos OS Release 22.3R1, 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: After you install a Junos OS Release 22.3R1 jinstall package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add no-validate` command and specify the jinstall package that corresponds to the previously installed software.

NOTE: Most of the existing `request system` commands are not supported on routers with 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:

- 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 example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 9: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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.

Upgrading a Router with Redundant Routing Engines

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

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

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

Downgrading from Release 22.3R1

To downgrade from Release 22.3R1 to another supported release, follow the procedure for upgrading, but replace the 22.2R1 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

These release notes accompany Junos OS Release 22.3R1 for the NFX Series Network Services Platforms. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R1 for NFX.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R1 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.

Interfaces

- On NFX250 devices, the LACP subsystem is not started automatically when dc-pfe process is restarted. PR1583054

Virtual Network Functions (VNFs)

- The NFX350 device stops responding after you configure VNF with SRIOV interfaces. Also, JDM becomes unreachable. PR1664814

Resolved Issues

IN THIS SECTION

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

General Routing

- On NFX250 device, core files are dumped into the device when you delete vmhost VLANs. PR1637649

Routing Protocols

- The BSR information might not be flooded over NG-MVPN. PR1664211

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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, 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 example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 10: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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.

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

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

Basic Procedure for Upgrading to Release 22.3

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 22.3R1:

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 PTX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

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

Interfaces

- **Support for IS-IS BFD-enabled sub-TLV (MX2010, MX2020, PTX10000, PTX10008, and PTX10016)**—Starting in Junos OS Release 22.3R1, the strict BFD feature allows IS-IS to converge only when BFD is up, and it sends the `UP` notification to IS-IS. We've introduced a new state in the IS-IS adjacency state machine (`InitStrictBFD` state) to indicate the agreement between routers to support strict BFD. We've also added a new BFD IS-IS Hello (IIH) PDU TLV in IS-IS hello packets.

  If BFD is unstable, to prevent the traffic from being compromised until the IS-IS adjacency timer expires, configure the hold-down interval (in milliseconds). This configuration delays sending the `UP` notification to the BFD client. After the BFD is up, the hold-down interval starts, and upon expiration, a BFD `UP` notification is sent to IS-IS so that IS-IS can start forming an adjacency.

  We've added the following statements for this feature:

  - `strict-bfd` at the `[edit protocols isis interface` *`name`* `level` *`level`* `]` hierarchy level.
  - `holddown-interval` at the `[edit protocols isis interface` *`interface`* `family inet bfd-liveness-detection]` hierarchy level.

  [See Configuring BFD, interface (Protocols IS-IS), and bfd-liveness-detection (Protocols IS-IS).]

Junos Telemetry Interface

- **BGP policy sensor upgrade (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10002, and vRR)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports data model

openconfig-bgp-policy.yang version 6.0.2 (upgraded from version 4.0.1). JTI also supports new BGP policy sensors.

[See Telemetry Sensor Explorer.]

- **Support for MPLS RSVP-TE sensors (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, and PTX10002)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports data model **openconfig-mpls-rsvp.yang** version 4.0.0. It supports new RSVP-TE sensors.

  [See Telemetry Sensor Explorer.]

- **Support for MPLS OpenConfig configuration and sensors (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, and PTX10002)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports the following data models:

  - **openconfig-mpls.yang** version 3.2.2
  - **openconfig-mpls-types.yang** version 3.2.1
  - **openconfig-mpls-te.yang** version 3.2.2
  - **openconfig-mpls-static.yang** version 3.2.2

  JTI supports the following OpenConfig configurations:

  - MPLS global
  - MPLS `named-explicit-path`
  - MPLS tunnels

  JTI supports the following state groups:

  - MPLS tunnels
  - MPLS `named-explicit-path`
  - MPLS static `label-switched-path`
  - MPLS-TE interface attributes
  - MPLS tunnel state counters (dependent on the Packet Forwarding Engine)

  [See Telemetry Sensor Explorer and Mapping OpenConfig MPLS Commands to Junos Configuration.]

- **INITIAL_SYNC enhancement for FIB streaming (MX240, MX960, MX2010, MX2020, PTX1000, PTX5000, and PTX10008)**—Junos OS Release 22.3R1 introduces improved performance time for the INITIAL_SYNC of telemetry statistics. This enhancement applies to subscription requests for the top-

level sensor path **/network-instances/network-instance/afts**. The INITIAL_SYNC feature gives the collector a complete view of the current state of every field on the device for that sensor path.

[See Enabling "INITIAL_SYNC" Subscription Mode through gNMI.]

- **Sensor for LSP name of MPLS next hops (MX240, MX960, MX2020, PTX1000, and PTX5000)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports the **/network-instances/network-instance/afts/next-hops/next-hop/state/lsp-name** sensor. This sensor will stream the LSP name associated with the nexthop.

  [See Telemetry Sensor Explorer.]

- **Support for VLAN sensors (ACX5448, ACX5448-M, ACX5448-D, and ACX710 routers, EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC and EX9208 switches, MX204, MX240, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2010, MX2020, PTX10008, and PTX10016 routers and vMX)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports the data model **openconfig-vlan.yang** version 3.2.1, including sensor support to stream VLAN and MAC- limit operational states through telemetry.

  [See Telemetry Sensor Explorer.]

Network Management and Monitoring

- **HMC fatal error SNMP trap (QFX10002-36Q, QFX10002-60C, QFX10002-72Q, QFX10008, QFX10016, PTX1000, PTX10002-60C, PTX10008, and PTX10016)**—Starting in Junos OS Release 22.3R1, the listed devices send SNMP trap messages from the SNMP agent to the SNMP manager whenever a Hybrid Memory Cube (HMC) fatal error occurs and gets cleared.

  We've added the following traps to detect the HMC fatal errors:

  - *jnxASICExternalMemTraps* and *jnxASICExternalMemOKTraps* at the *jnxTraps* hierarchy level. The *jnxASICExternalMemTraps* and *jnxASICExternalMemOKTraps* traps get triggered when there is an ASIC external memory error.

  - *jnxHmcFatal* at the *jnxASICExternalMemTraps* hierarchy. The *jnxHmcFatal* trap triggers when it detects that the specified HMC on a specific FPC has failed.

  - *jnxHmcOK* at the *jnxASICExternalMemOKTraps* hierarchy level. The *jnxHmcOK* trap triggers when the specified HMC on a specific FPC has recovered from the failure.

  The HMC SNMP traps are raised for fatal HMC errors only. The *jnxHmcOK* trap is triggered only once for each FPC, although several fatal HMC errors are triggered and then cleared.

[See SNMP MIBs and Traps Supported by Junos OS.]

OpenConfig

- **Support for OpenConfig VLAN model (ACX5448, MX10003, PTX10008, QFX5110, and QFX10002)**—Starting in Junos OS Release 22.3R1, we support the OpenConfig VLAN data model **openconfig-vlan.yang**, version 3.2.1. You can use paths for configuration and for streaming of operational state data.

  [For operational state paths, see Telemetry Sensor Explorer. For configuration, see Mapping OpenConfig VLAN Commands to Junos Configuration.]

- **Support for OpenConfig BFD configuration and state (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, and PTX10002)**—Starting in Junos OS Release 22.3R1, we support OpenConfig configuration and state support for BFD. Use BFD telemetry data to detect failures in the forwarding path between two adjacent routers.

  [See Mapping OpenConfig Interface Commands to Junos Configuration and Telemetry Sensor Explorer.]

- **OpenConfig IS-IS configuration support (ACX5448, ACX710, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX3000, PTX10002, and PTX10003)**—Starting in Junos OS Release 22.3R1, we support IS-IS configuration using OpenConfig.

  [See Mapping OpenConfig ISIS Commands to Junos Configuration.]

Routing Protocols

- **Fast lookup of origin and neighbor ASs (MX480, MX960, MX10008, PTX1000, PTX10002, PTX10008, PTX10016, QFX10008, and vRR)**—Starting in Junos OS Release 22.3R1, you can use the new `asregex-optimize` configuration statement at the `[edit policy-options defaults]` hierarchy level to perform a fast lookup of origin and neighbor autonomous systems (ASs). This optimization supports very large AS-Path regular expressions (typically as-path-group configuration) when the objective is to match neighboring ASes, or origin ASes.

  [See Improve the Performance of AS Path Lookup in BGP Policy.]

- **IS-IS flood optimization (MX960, MX2008, MX2010, MX2020, PTX10002, PTX10008, and PTX10016)**—Starting in Junos OS Release 22.3R1, you can rate-limit the IS-IS link-state PDUs that are retransmitted on parallel interfaces toward the same peer. This feature optimization prevents frequent drops in IS-IS hello protocol data units (PDUs) and subsequent adjacency reset. The optimizations also involve changes to the LSP transmission queues to avoid longer delays for frequently updated LSPs.

- **Strip and replace BGP private-AS path (ACX710, JRR200, MX480, PTX10001, QFX5220, and QFX10003)**—In Junos OS Release 22.3R1, we have introduced the `strip-as-path` policy option that removes the incoming autonomous system (AS) path as part of the import policy for a BGP session and replaces the received autonomous system (AS) path with the receiving router's local AS number for the receiving session. Note that the local AS number may be different from the number configured under `autonomous system` in the `[edit routing-options]` hierarchy.

  If you need to normalize externally injected routes, you can use this policy option for the incoming autonomous system (AS) path so that it may be used similarly to routes that originate solely within the fabric. The new `strip-as-path` policy option has no impact on the BGP export policy.

  You can configure the `strip-as-path` option under `policy-options then` clause:

  ```
  set policy-options policy-statement do-strip term a then strip-as-path
  ```

  [See Autonomous Systems for BGP Sessions.]

What's Changed

IN THIS SECTION

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

General Routing

- **JNP10K-PWR-DC2 power supplies installed in PTX10008 and PTX10016 routers display as online when the power supplies are switched off**—JNP10K-PWR-DC2 power supplies installed in PTX10008 and PTX10016 routers in which Junos OS Release 21.4R1 or Junos OS Evolved Release 21.4R1 is installed display as online in the output of the command 'show chassis environment psm' when the input power feeds are connected, but the power switch on the power supplies are switched off.

User Interface and Configuration

Support for temperature sensor (PTX10001-36MR)—We support the temperature sensor statement at the `edit chassis cb` hierarchy level. You can use the temperature sensor statement to increase the fan speed and customize the temperature threshold. We recommend certain values for ZR and ZR-M modules to work which helps the temperature to remain within the thresholds.

[See temperature-sensor.]

Known Limitations

IN THIS SECTION

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

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

General Routing

- Whenever the underlay interface flaps for 1K legacy GR-tunnels, BGP establishment over these tunnels may take ~8 to 10 minutes.PR1614179

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` statement. PR1568757

Open Issues

IN THIS SECTION

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

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

General Routing

- The issue occurs on Junos OS routers and switches, with LACP enabled. Deactivating a remote aggregated Ethernet member link makes the local member link move to LACP detached state and cause traffic drops on that member link. The same scenario applies when you add a new member link and not configure the other end of that link with LACP. PR1423707
- The script attempts an unsupported configuration and then hits the maximum threshold for the given platform. PR1555159
- On PTX platforms, when you configure Inline Jflow and set high sampling rate (more than 4000 per second), you might observe high CPU utilization. It might also result in relevant impacts on traffic analysis and billing.PR1569229
- The issue occurs on ACX, PTX, and QFX platforms (PTX10002, PTX10003, PTX10008, PTX10016, QFX10002, QFX10003, QFX10008, QFX10016, and ACX6360). If you enable protocols l2circuit and channel tcc for providing L2 transaction, IS-IS connection through the L2 domain might fail and cause traffic loss. PR1590387
- On PTX10002-60C and QFX10002-60C, after a system reboot, you might see the `FPC 0 Major Errors` alarm due to a rare timing issue. The issue might cause the host path traffic to drop. It is a rare issue and does not always happen during reboot. Perform `request vmhost reboot` for recovery. PR1613229
- V6 default route will not get added after successful DHCPv6 client binding on PTX1000 router during ZTP. PR1649576

- Presence of consistent hash/resiliency feature in the running configuration causes the system to take much longer to converge, in case of a churn. PR1652750
- You might not receive DHCPACK at ztp-server after zeroize of the device (client). PR1658287
- You might observe **vmcore.lockdown1-fpc1.12.tar** on PTX5000. PR1668229
- Junos OS Release 20.2R1 and later releases have introduced firmware version for PHY chip on some PIC models. After that migration, some of the 100GE ports on PIC or its peer devices would see PCS and framing errors.PR1669267

Routing Protocols

- If you configure any platforms with Micro BFD on member links of the LAG/aggregated Ethernet interface, BFD Session state in Routing Engine remains as `UP` always, even though PEER device has ceased.PR1675921

Resolved Issues

IN THIS SECTION

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

Class of Service (CoS)

- The default code-point aliases and respective CoS value Bit patterns are inconsistent with Junos in Junos OS Evolved. PR1667404

Interfaces and Chassis

- The FPCs might not come online after the USB upgrade method. PR1637636
- You might observe `reth1 interface down and DCD` core files on node1 during test on 22.2R2 image. PR1657021

General Routing

- The Routing Engine goes into a fault state if you execute `request node power-on` CLI command while the node is powering off. PR1589737
- `/interfaces/interface/subinterfaces/subinterface/state/counters` are not exported during initial sync for on-change. PR1620160
- In some reload scenarios, config-sync failure might trigger a major alarm `Application config-sync fail on node Re1`. The failure might cause configuration mismatch between primary Routing Engine and backup Routing Engine. PR1629952
- ON_CHANGE telemetry does not work for `backplane-facing-capacity` sensors. PR1635606
- KRT queue entries are stuck during Routing Engine switchover when backup RPD is not yet ready. PR1641297
- On Junos PTX/QFX platforms, silent drop of traffic might occur after interface flaps. PR1645488
- EDAC errors might not generate alarm until you reboot the FPC.PR1646339
- mac-vrf does not support mac limit configuration. PR1647327
- BGP Sensor `/bgp-rib/afi-safis/afi-safi/ipv4-unicast/loc-rib/`is not available as a 'periodic' sensor. PR1649529
- Junos OS: PTX Series: FPCs might restart unexpectedly upon receipt of specific MPLS packets with certain multi-unit interface configurations (CVE-2022-22202). PR1649586
- IRP memory parity issue might result in traffic loss on Junos PTX and QFX10000 platforms. PR1650217
- PCS faulty blocks count will increment after Junos software upgrade to Junos OS Release 20.2R1 or above. PR1651526
- The traffic with EtherType 0X88FC might get corrupted. PR1651703

- The jvision sensors might not get reset after you restart routing, resulting in verification failure. PR1652372
- Configuring gre-key in firewall filter might breaks the DSCP classification. PR1652762
- SRv6 END.DT46 and END.DT4 configuration might not be supported. PR1655518

MPLS

- Premature RSVP Path Error BW-Unavailable originated by PLR. PR1670638
- The rpd crash occurs with Container LSPs. PR1672804
- The traffic might drop when you set the link-state protocol with the least preference to active, and the CSPF algorithm fails. PR1677930

Multicast

- Silent drop in traffic might be seen due to next-hop install failure on Junos PTX platforms. PR1653920

Migration, Upgrade, and Downgrade Instructions

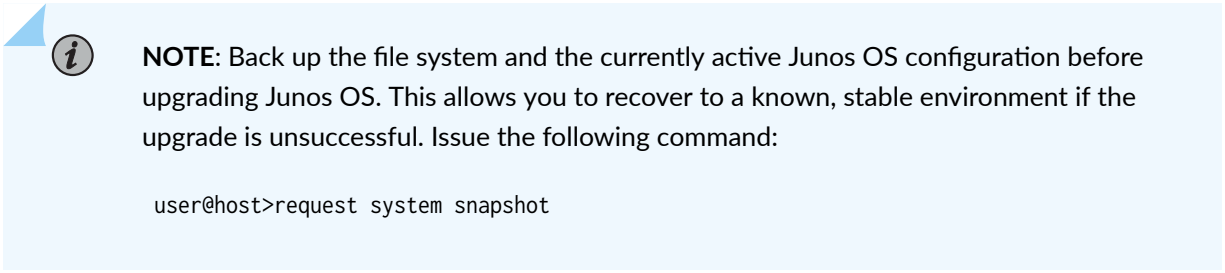
IN THIS SECTION

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

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

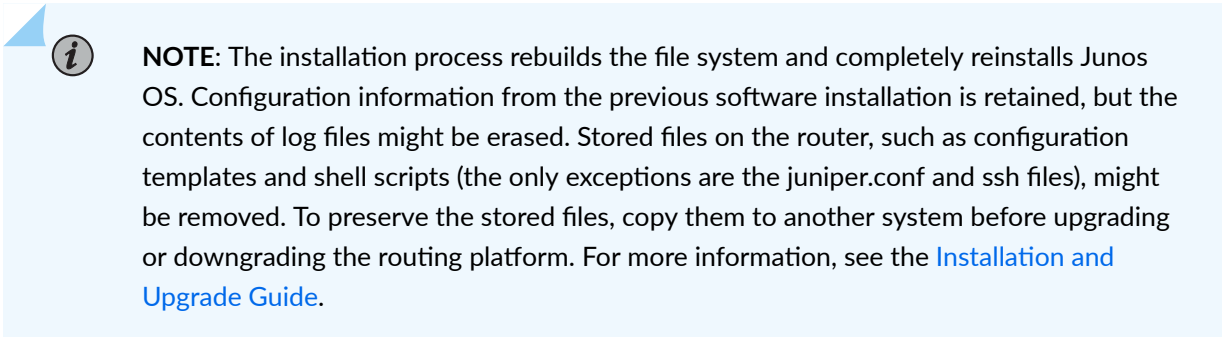
Basic Procedure for Upgrading to Release 22.3

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

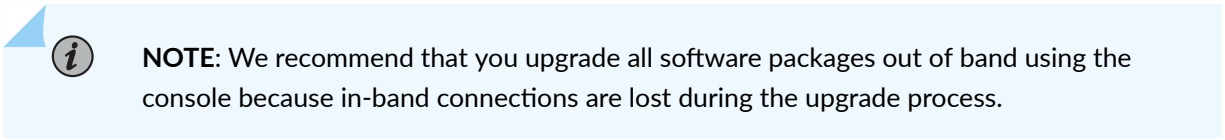


NOTE: Back up the file system and the currently active Junos OS configuration before upgrading Junos OS. This allows you to recover to a known, stable environment if the upgrade is unsuccessful. Issue the following command:

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



NOTE: The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the router, such as configuration templates and shell scripts (the only exceptions are the juniper.conf and ssh files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see the Installation and Upgrade Guide.



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

To download and install Junos OS Release 22.3R1:

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

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

2. Select the name of the Junos OS platform for the software that you want to download.

3. Select the release number (the number of the software version that you want to download) from the Release drop-down list to the right of the Download Software page.

4. Select the `Software` tab.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new jinstall package on the router.

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

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

```
user@host> request system software add validate reboot source/junos-install-ptx-
x86-64-22.3R1.9.tgz
```

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

```
user@host> request system software add validate reboot source/junos-install-ptx-
x86-64-22.3R1.9-limited.tgz
```

Replace the source with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: You need to install the Junos OS software package and host software package on the routers with the RE-PTX-X8 Routing Engine. For upgrading the host OS on this router with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.

NOTE: After you install a Junos OS Release 22.3 jinstall package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the jinstall package that corresponds to the previously installed software.

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 11: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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.

Upgrading a Router with Redundant Routing Engines

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

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

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

Junos OS Release Notes for QFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for QFX Series switches.

Interfaces

- **Support for Flexible Ethernet services (QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 22.3R1, you can configure Flexible Ethernet services encapsulation on the QFX10000 line of switches. This configuration ensures that the switches support multiple logical interfaces on the same physical interface mapped to the same bridge domain.

  NOTE: The QFX10002-60C switches do not support this feature.

  [See Flexible Ethernet Services Encapsulation.]

- **Support for 128 Down-Link Interfaces during Uplink Failure Detection (QFX5120-32C and QFX5120-48Y)**—Starting in Junos OS Release 22.3R1, the number of down-link interfaces supported during the Uplink Failure Detection is increased from 48 down-link interfaces to 128 down-link interfaces.

  [See Network Management and Monitoring Guide].

Juniper Extension Toolkit (JET)

- **Use JET Interfaces Service API to reduce operational time of port bounces (EX Series, QFX Series, and SRX Series)**—A port bounce is the act of disabling and re-enabling a physical interface. Starting in Junos OS Release 22.3R1, you can use the JET Interfaces Service API to perform a port bounce. To disable the port without using the CLI, set the `disable` attribute in the Interfaces Service RPC message to 1 for that port. To remove that configuration and re-enable the port, set `disable` to 0.

  When you set `disable` to 1 in the RPC message, the API disables the port regardless of the CLI or API configuration for that port. When you set `disable` to 0, the API deletes the setting of the `disable` attribute from the API configuration, so the configuration for the port reverts to the previous configuration.

  Details of the Interfaces Service API are in the **jnx_interfaces_service.proto** file in the JET package.

  [See Overview of JET APIs.]

Network Management and Monitoring

- **HMC fatal error SNMP trap (QFX10002-36Q, QFX10002-60C, QFX10002-72Q, QFX10008, QFX10016, PTX1000, PTX10002-60C, PTX10008, and PTX10016)**—Starting in Junos OS Release 22.3R1, the listed devices send SNMP trap messages from the SNMP agent to the SNMP manager whenever a Hybrid Memory Cube (HMC) fatal error occurs and gets cleared.

  We've added the following traps to detect the HMC fatal errors:

- *jnxASICExternalMemTraps* and *jnxASICExternalMemOKTraps* at the *jnxTraps* hierarchy level. The *jnxASICExternalMemTraps* and *jnxASICExternalMemOKTraps* traps get triggered when there is an ASIC external memory error.
- *jnxHmcFatal* at the *jnxASICExternalMemTraps* hierarchy. The *jnxHmcFatal* trap triggers when it detects that the specified HMC on a specific FPC has failed.
- *jnxHmcOK* at the *jnxASICExternalMemOKTraps* hierarchy level. The *jnxHmcOK* trap triggers when the specified HMC on a specific FPC has recovered from the failure.

The HMC SNMP traps are raised for fatal HMC errors only. The *jnxHmcOK* trap is triggered only once for each FPC, although several fatal HMC errors are triggered and then cleared.

[See SNMP MIBs and Traps Supported by Junos OS.]

OpenConfig

- **Support for OpenConfig VLAN model (ACX5448, MX10003, PTX10008, QFX5110, and QFX10002)**—Starting in Junos OS Release 22.3R1, we support the OpenConfig VLAN data model **openconfig-vlan.yang**, version 3.2.1. You can use paths for configuration and for streaming of operational state data.

  [For operational state paths, see Telemetry Sensor Explorer. For configuration, see Mapping OpenConfig VLAN Commands to Junos Configuration.]

Routing Protocols

- **IS-IS adjacency through VXLAN (QFX10002-60C, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 22.3R1, we support IS-IS for multivendor networks. IS-IS logical link control (LLC) packets that are encapsulated in a VXLAN tunnel now have their VLAN tags removed by default.

  If you want the VLAN tags to be preserved and carried through the VXLAN tunnels, use the `set routing-instances` *`routing-instance-name`* `vlans` *`vlan-name`* `vxlan encapsulate-inner-vlan` command.

  [See encapsulate-inner-vlan.]

- **Fast lookup of origin and neighbor ASs (MX480, MX960, MX10008, PTX1000, PTX10002, PTX10008, PTX10016, QFX10008, and vRR)**—Starting in Junos OS Release 22.3R1, you can use the new `asregex-optimize` configuration statement at the `[edit policy-options defaults]` hierarchy level to perform a fast lookup of origin and neighbor autonomous systems (ASs). This optimization supports very large AS-Path regular expressions (typically as-path-group configuration) when the objective is to match neighboring ASes, or origin ASes.

  [See Improve the Performance of AS Path Lookup in BGP Policy.]

- **Strip and replace BGP private-AS path (ACX710, JRR200, MX480, PTX10001, QFX5220, and QFX10003)**—In Junos OS Release 22.3R1, we have introduced the `strip-as-path` policy option that removes the incoming autonomous system (AS) path as part of the import policy for a BGP session and replaces the received autonomous system (AS) path with the receiving router's local AS number for the receiving session. Note that the local AS number may be different from the number configured under `autonomous system` in the `[edit routing-options]` hierarchy.

  If you need to normalize externally injected routes, you can use this policy option for the incoming autonomous system (AS) path so that it may be used similarly to routes that originate solely within the fabric. The new `strip-as-path` policy option has no impact on the BGP export policy.

  You can configure the `strip-as-path` option under `policy-options then` clause:

  ```
  set policy-options policy-statement do-strip term a then strip-as-path
  ```

  [See Autonomous Systems for BGP Sessions.]

Additional Features

We've extended support for the following features to these platforms.

- **Supported transceivers, optical interfaces, and direct attach copper (DAC) cables**. Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update this tool and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

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

General Routing

- OpenConfig container names for Point-to-Multipoint per interface ingress and egress sensors are modified for consistency from "signalling" to "signaling".
- **New ARP and NDP packet classification (QFX10002, QFX10016, and QFX10008)**—We've introduced two control plane classes for ARP and NDP packets received over VTEP interface. When your device identifies a packet as ARP or NDP, it performs an ingress port check which verifies whether the VTEP interface receives these packets. If VTEP interface receives the packet, datapath re-writes the control plane class to the newly defined values. Based on this new control plane class, the system performs the remaining packet processing and forwards the packets toward the host path. The system adds a separate DDoS policer to this ARP traffic, which ensures that the ARP traffic is not triggering underlay ARP DDoS violation.

MPLS

- Starting with Junos OS and Junos Evolved release 21.4R3 a CSPF LSP uses a new instance ID when attempting to re-signal a down LSP.

Known Limitations

IN THIS SECTION

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

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

General Routing

- Junos OS does not support the Unified ISSU on QFX5120-48Y switches if there is a change in the Cancun versions of the chipset SDKs between the releases. This is a product limitation as change in the Cancun firmware leads to the chip reset and hence ISSU is impacted. The Cancun versions in the chipset SDKs should be the same between two JUNOS OS releases for ISSU to work. PR1634695
- When EVPN-VxLAN tunnel gets established over IPv6 underlay, the encapsulated packets emitted out of leaf node (QFX10000) might have UDP checksum zero. This is the default behavior of all IPv6 tunneled UDP packets and it is allowed as per RFC6936. PR1656363

Infrastructure

- When upgrading from Junos OS release 21.2 prior and later, validation and upgrade fails. You must use the `no-validate` command while upgrading. PR1568757

Open Issues

IN THIS SECTION

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

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

Class of Service (CoS)

- On QFX5100 switches, traffic might not get classified based on a fixed classifier in MPLS in the VXLAN scenario. PR1650051

Layer 2 Ethernet Services

- The DHCP client configuration comes from two places that is, AIU script and vsdk sandbox. The DHCP client configuration comes from AIU script has the serial ID in the vendor ID where as the default configuration from sandbox does not have. There is no impact on functionality or service. PR1601504

Layer 2 Features

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

Platform and Infrastructure

- On all Junos platforms, while using source-address NTP configuration parameter and issue the `set ntp date` command from the CLI, packets gets sent with the source address of the outgoing interface rather than the manually configured IP address. Typically, the manually configured IP address would be a loopback address. The problem does not apply to automatically generated NTP poll packets.PR1545022
- On QFX5100 line of switches, inserting or removing optics on a port might cause a Packet Forwarding Engine Manager CPU spike and an eventual microcode failure. PR1372041
- VXLAN VNI (multicast learning) scaling on QFX5110 devices, traffic issue occurs from VXLAN tunnel to Layer 2 interface. PR1462548
- 5M DAC connected between QFX10002-60C devices does not link up. But with 1M and 3M DAC this interop works as expected. The QFX10002-60C or traffic generator the same 5M DAC works seamlessly. There seems to be certain SI or link level configuration on the QFX10002-60C devices, which needs to be debugged with the help from HW and SI teams and resolved. PR1555955

- To avoid the additional interface flap, interface hold time needs to be configured. PR1562857
- Pim VXLAN does not work on TD3 chipsets enabling VXLAN flexflow after Junos OS release 21.3R1. Customers Pim VXlan or data plane VXLAN can use Junos OS release 21.3R1. PR1597276
- On QFX5100 switches, optical power appers after you detach and attach the QSFP on a disable interface. PR1606003
- On QFX5120-48Y devices, when a scaled configuration and baseline configurations gets loaded multiple times one after other without much wait time in between then traffic or protocols on pure Layer 3, interfaces might behave in an undefined or unexpected manner. PR1612973
- On QFX10002-60C switches after the system gets rebooted, the `FPC 0 Major Errors` alarm might appear due to a rare timing issue. The issue could cause the host path traffic to get dropped. It is a rare issue and does not always happen during reboot. You must use the `request vmhost reboot` command for recovery. PR1613229
- The backup FPC loses their connection to primary when you add the new members to the VCF (Virtual Chassis Fabric). PR1634533
- On all devices running Junos OS, where this is a high BGP scale with flapping route and the BGP Monitoring Protocol (BMP) collector or station is very slow, the rpd process might crash due to memory pressure. PR1635143
- When you enable MACSEC and VRRP on QFX5120 Virtual Chassis, the MACSEC sessions flaps at random times. Without VRRP this issue does not occur. PR1640031
- On all QFX5100 Virtual Chassis platforms, after the reboot, Virtual Chassis port (VCP) ports might not establish a VCP connection and Cyclic Redundancy Check (CRC) errors gets generated. PR1646561
- On QFX switches, IPv6 traffic output byte (ipv6-transit-statistics) would not be in expected range as per traffic generator status. PR1653671
- QFX5100-24Q Virtual Chassis in the `Unstable` state for 3 to 7 minutes causes traffic loss. PR1661349
- When the remote end server or system reboots, QFX5100 switches port with SFP-T 1G inserted might go into the `Hung` state and remain in that state even after the reboot is complete. This might affect traffic after the remote end system comes online and resumes traffic transmission. PR1665800
- Each locally learned ARP/ND nexthop requires unique fabric token from Kernel. This unique token maps to physical address in HW and this address points to EDF memory for the ARP/ND nexthops. Token pool in kernel is also used by different features like flood nexthops, arp/ndp nexthops. Token usage has increased as tokens are now used by IRB interfaces and default mesh groups also. 96,000 ARP/ND scale might not be achievable always. It is recommended to scale upto 95,000 ARP/ND. PR1673626

- On QFX5100 devices, media type for SFP+-10G-CU1M and SFP-T cables gets displayed as Fiber. PR1570555
- On QFX5110 Virtual Chassis, FPC might gets disconnected with 24000 DHCPv6 relay scaling after the traffic stops. The `pfe_listener_disconnect` error message gets generated. PR1594748
- On QFX10008 devices, statistics for multicast packets is not as expected as the packets has Layer 2 header strips during replication in the Packet Forwarding Engine because of which it is not forwarded to the next hop. PR1678723

Resolved Issues

IN THIS SECTION

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.

Chassis Clustering

- GTP control packets might be incorrectly dropped or passed if there is more than one APN IMSI filter configured. PR1673879

EVPN

- The spine might have stale vtep entry for the ESI even though the host MAC does not get advertised by the leaf. PR1648368
- ARP or NS response to anycast IRB might fail due to the missing MAC-IP entry. PR1650202
- BUM traffic might be silently discarded for the ESI configured CE interface flap. PR1669811

Forwarding and Sampling

- The `jnxL2aldMacNotificationMIBObjects` does not work on certain Junos OS platforms. PR1647660

Interfaces and Chassis

- VRRP flaps between MC-LAG peers when you delete VLAN on the MC-AE interfaces. PR1579016
- Traffic loss might be seen for the MAC addresses learned on the ICL interface. PR1639713
- Incorrect configuration and rollback might cause issues with ARP learning between ICL interface and local MC-AE interfaces. PR1648271
- The MAC address might be learned over the incorrect interface in the MC-AE scenario. PR1658742

Network Management and Monitoring

- VTEP might report a high speed on the sub-interface, causing SNMP alarms. PR1651774

Platform and Infrastructure

- On QFX10008 and QFX10016 switches, the chassisd process generates `Cannot read hw.chassis.startup_time value: m` error message every 5 seconds. PR1603588
- The packet drop might be seen when packet size exceeds 9000 MTU. PR1615447

- The BFD session might flap in a scaled scenario. PR1621976
- The interface on the peer device might remain up even after disabling the 10G interface on the Juniper device. PR1629637
- Multicast traffic received from an external source might not be sent to the multihomed listener interfaces. PR1631249
- On QFX5120-48Y switches, traffic loss might be observed when there is a link flap. PR1634495
- Routes might be slow to install in the LPM table. PR1635887
- Multicast traffic received on the INET interface might be dropped. PR1636842
- The Packet Forwarding Engine might crash while removing the port from a VLAN. PR1637013
- MACsec traffic gets silently discarded when you perform a back-to-back graceful switchover. PR1637822
- QFX5220 switches might experience system reboot or shutdown in rare cases. PR1638961
- Traffic might get silently discarded after the interface flaps. PR1645488
- On QFX5000 switches, an interface might be detached from LACP when you configure VLAN tagging in the EVPN-VXLAN scenario. PR1645929
- VXLAN Tunnel termination fails due to a change in the configuration. PR1646489
- The CLNP traffic tunneled through the EVPN-VXLAN fabric might get dropped. PR1648078
- OSPF control packets might get dropped due to the flow check function in the interoperability case. PR1648272
- On QFX5100 Virtual Chassis, the local-minimum-links feature does not work as expected. PR1649637
- In the EVPN-VXLAN environment, non-VXLAN traffic might be dropped if the VXLAN and non-VXLAN traffic share the same ECMP next-hop. PR1649841
- Traffic might be lost with the Virtual-Router. PR1650335
- L2PT configuration on a transit switch in a Q-in-Q environment breaks L2PT. PR1650416
- The local-bias might stop working after the device reboots. PR1651151
- Transit traffic might get dropped and protocols might be down when you modify the firewall filters. PR1651546
- The traffic with ether type 0X88FC might get corrupted. PR1651703

- The inner tag (C-tag) value might get modified to zero for egress traffic when you copy the inner tag values o the outer tag (S-tag). PR1652976
- Port might be down after inserting specific SFP. PR1653723
- The ARP might not resolve with the native-VLAN configuration. PR1654215
- LACP sent IN SYNC to server facing interface when core-isolation is in effect. PR1654459
- FEC link goes down after disabling or enabling interface. PR1657534
- TOS(DSCP+ECN) bits do not get copied from the Inner Layer 3 header to the outer VXLAN header. PR1658142
- Valid software licenses might not be in synchronization between members in the Virtual Chassis. PR1658913
- The multipath route might be missing when you configure multipath. PR1659255
- The secondary PTP device does not lock the clock with the primary PTP device. PR1659453
- Traffic might drop when a VXLAN port recovers from a failure. PR1659533
- On QFX10000 switches, configuration of IGMP group range might result in traffic loss. PR1659732
- MACsec session configured over the physical interface might be down when you configure a logical interface on disabled/deactivated FD. PR1660070
- After changing the MTU on an aggregated interface along with IRB the kernel might crash. PR1660208
- OSPF flow check function violates RFC6864. PR1660369
- On QFX10008 or QFX10016 switches, the spmb0 Cell drops on sib 'x' pf 'x' errors gets generated without generating any alarms. PR1660699
- CoS might not get applied on the Virtual Chassis ports. PR1660787
- BUM traffic might loop post adding or removing EVPN-VXLAN FRR configuration. PR1662515
- On QFX5100 and QFX5110 switches, the IPv6 ND packets might be dropped. PR1662707
- Verification of status for the BFD session goes in to the `Up` state while checking the BFD session. PR1663790
- ALB status does not get displayed in the CLI. PR1663881
- On QFX5000 switches, duplicate packets might occur in the multihomed scenario in an EVPN-VxLAN fabric when unicast ARP packets are received. PR1665306

- Static MACs are not programmed after reboot, resulting in floods of unicast traffic. PR1666399
- Multihop BFD sessions might remain in the `Down` status in the inline mode. PR1667751
- Shaping-rate does not take 20 bytes of overhead into account. PR1667879
- On specific QFX5000 switches, member links might reduce their configured speed when the other side does not have auto-negotiation disabled. PR1669436
- FPC1 gets disconnected after in-service-software-upgrade (ISSU) and before switchover while checking ISSU status. PR1669702
- On QFX5120-48YM devices, ECN bits do not get copied to VXLAN tunnel header at the encapsulation node. PR1672308
- VLAN translation programming gets deleted from the Packet Forwarding Engine upon deleting the a member interface for LAG. PR1676772
- The rpd process might crash when you deactive the EVPN protocol. PR1659786
- The dcpfe process might generate core files and FPC might crash after line card reboots or switchovers. PR1670240
- The BFD packets drops in an EVPN-VxLAN scenario due to incorrect Layer 3 offset being set in the host path. PR1674116

Routing Protocols

- PIM `accept-remote-source` command configuration removal. PR1593283
- Routing Process Daemon (rpd) crashes and restarts when a specific timing condition is hit with BGP configuration. PR1659441
- A policy with a policy action `community` configuration might not work. PR1660424
- Packets get dropped on the Server leaf in the EVPN-VXLAN with OISM. PR1665791
- The mcsnoopd process gets restarted and will again learn the states after core. PR1672488
- Traffic drops due to the generation of the FPC core, which makes the system unstable. PR1678016

User Interface and Configuration

- On QFX5120 switches, the l2ald process generates core file at `?0x0000000000676fed` in `l2ald_config_read_bridgedomain (insttype= optimized out>, obj=0x0, lr=0x0, rtt=0x3317010)` at `l2ald/l2ald_config_bd.c:2607` after loading test configurations. PR1652605

- The `gethostbyname : Host name lookup failure` error message gets generated during commit. PR1673176

VPNs

- On QFX10000 switches, auto-RP goes down after some time in the NGMVPN scenario. PR1617620

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

Upgrading Software on QFX Series Switches

When upgrading or downgrading Junos OS, always use the jinstall package. Use other packages (such as the jbundle package) only when so instructed by a Juniper Networks support representative. For

information about the contents of the jinstall package and details of the installation process, see the Installation and Upgrade Guide and Junos OS Basics in the QFX Series documentation.

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

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

   The Junos Platforms Download Software page appears.

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

3. Select **22.3** in the Release pull-down list to the right of the Software tab on the Download Software page.

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 22.3 release.

   An Alert box appears.

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

   A login screen appears.

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

7. Download the software to a local host.

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

9. Install the new jinstall package on the device.

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

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

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-22.3-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 22.3 `jinstall` package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

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

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

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

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

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

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

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-20.4R1.9.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" on page 167
- "Upgrading the Software Using Unified ISSU" on page 167

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, 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 example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 12: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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 SRX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for the SRX Series Services Gateways. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for SRX Series devices.

High Availability

- **Multinode High Availability (SRX5400, SRX5600, and SRX5800 with SPC3, IOC3, SCB3, SCB4, and RE3; SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 22.3R1, we extend Multinode High Availability support to SRX4600, SRX4200, SRX4100, and SRX1500 devices and vSRX 3.0 instances. In this release, we support the following network deployment modes:
  - Layer 3 network
  - Default gateway
  - Hybrid network
  - Public cloud deployment (AWS)

  SRX Series devices with Multinode High Availability support firewall and advanced security services such as application security, Content Security, intrusion prevention system (IPS), firewall user authentication, NAT, and ALG. For the complete list of features supported with Multinode High Availability, see Feature Explorer.

[See Multinode High Availability.]

- **PKI-based link encryption (SRX5400, SRX5600, and SRX5800 with SPC3, IOC3, SCB3, SCB4, and RE3; SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 22.3R1, we support PKI-based link encryption for interchassis links (ICLs) in Multinode High Availability. PKI provides a way of verifying the identity of a remote site by using a digital certificate.

  You can now generate and store node-specific PKI objects such as local keypairs, local certificates, and certificate-signing requests on both nodes. You can generate, view, and clear node-specific certificates using the CLI commands with the `node-local` option.

  [See Multinode High Availability, request security pki node-local generate-key-pair, request security pki node-local generate-certificate-request, and show security pki node-local local-certificate.]

J-Web

- **Support for role-based access control (SRX Series)**—Starting in Junos OS Release 22.3R1, J-Web supports users' authentication and authorization based on their roles. When root, tenant, or logical-system users log in to J-Web, their roles and access permissions determine the J-Web menus they can access and the tasks they can perform. For logical system and tenant users, the J-Web UI does not display menus for the restricted features.
  [See About the Roles Page and Edit a Logical System.]

- **Support for metadata streaming, DNS security, and ETI (SRX Series)**—Starting in Junos OS Release 22.3R1, J-Web supports:

  - Encrypted traffic insights (ETI), which help you detect malicious threats that are hidden in encrypted traffic without intercepting and decrypting the traffic.
  - DNS Domain Generation Algorithm (DGA) detection, which facilitates in-line DNS query blocking and sinkholing on your security devices.
  - Security metadata streaming policy, which helps security devices to send the metadata and connection patterns of a network to Juniper ATP Cloud.

  [See Monitor DNS Security, Monitor Encrypted Traffic Insights, Metadata Streaming Policy, Metadata Streaming Profile, and Configure DNS Sinkhole.]

Juniper Extension Toolkit (JET)

- **Use JET Interfaces Service API to reduce operational time of port bounces (EX Series, QFX Series, and SRX Series)**—A port bounce is the act of disabling and re-enabling a physical interface. Starting in Junos OS Release 22.3R1, you can use the JET Interfaces Service API to perform a port bounce. To disable the port without using the CLI, set the `disable` attribute in the Interfaces Service RPC message to 1 for that port. To remove that configuration and re-enable the port, set `disable` to 0.

When you set `disable` to 1 in the RPC message, the API disables the port regardless of the CLI or API configuration for that port. When you set `disable` to 0, the API deletes the setting of the `disable` attribute from the API configuration, so the configuration for the port reverts to the previous configuration.

Details of the Interfaces Service API are in the **jnx_interfaces_service.proto** file in the JET package.

[See Overview of JET APIs.]

VPNs

- **Deprecated IPsec manual VPN configuration statement (SRX Series devices and vSRX instances that run the kmd process))**—Starting in Junos OS Release 22.3R1, we've deprecated the manual IPsec VPN (flow mode) configuration. Therefore, you cannot establish a manual IPsec security association through the [`edit security ipsec vpn` *`vpn-name`* `manual`] configuration hierarchy.

  [See manual (Security IPsec).]

- **Chassis Cluster HA control link encryption (SRX5000 line of devices with SPC3 card)**—Starting in Junos OS Release 22.3R1, we support Chassis Cluster HA control link encryption. The Chassis Cluster HA control link encryption protects traffic between the HA nodes using the trusted IPSec protocols.

  With Chassis Cluster HA link encryption tunnel, any security sensitive parameters or critical security parameters exchanged over the control link between the two chassis in chassis cluster mode are protected using IPSec. Using IPSec for internal communication between nodes, information such as, configuration information and IKE HA messages that passes through the chassis cluster link from the primary node to the secondary node is protected from active and passive eavesdropping.

  To activate Chassis Cluster HA control link encryption, use the below commands:

  - set groups node0 security ipsec vpn *<vpn-name>* ha-link-encryption
  - set groups node1 security ipsec vpn *<vpn-name>* ha-link-encryption

  [See Chassis Cluster HA Control Link Encryption, show security ipsec security-associations, show security ike security-associations, show security ipsec security-associations, show security ipsec statistics, clear security ike security-associations, and clear security ipsec security-associations.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series.

Platform and Infrastructure

- SRX Series devices does not drop session with server certificate chain more than 6.
- **from-zone and to-zone are optional when policy match is done for global policies (SRX Series)**—When you use match criteria to troubleshoot traffic problems for global policies, from-zone and to-zone need not be provided while performing the policy match.

  [See show security match-policies.]
- **sFlow configuration**—sFlow configuration is allowed only on et, xe, and ge interfaces in EVO-based platforms. All other interfaces are blocked for configuring sFlow on EVO platforms. A cli error will be thrown if sFlow is configured on any other interface other than et, xe or ge interface.

SSL Proxy

- **No session cache entry store during SSL session resumption (SRX Series Devices)**—When an SSL session attempts to re-initiates a full handshake and the server rejects that session resumption, the session cache does not store session information and remains empty. This issue is seen in a setup where a client device is using TLS1.1 version and the server is using TLS1.3 (maximum) version.

  In Junos OS Release 22.3R1, the session cache stores session information even when the session resumption is rejected, and you can see the session cache entries using the `show services ssl proxy session-cache entries summary` command.

Unified Threat Management (UTM)

- **Content filtering CLI updates (SRX Series and vSRX)**—We've the following updates to the content filtering CLI:
  - Trimmed the list of file types supported for content filtering rule match criteria. Instead of uniquely representing different variants of a file type, now only one `file-type` string represents all variants. Hence, the `show security utm content-filtering statistics` output is also updated to align with the new file types available in the rule match criteria.
  - Renamed the content filtering security logging option `seclog` to `log` to match with the Junos OS configuration standard.
  - Rephrased the `reason` string associated with content filtering security log message.

[See show security utm content-filtering statistics, content-filtering (Security Feature Profile), and content-filtering (Security UTM Policy).]

VPLS

- **No output byte increment on VPLS interface when configured with output filter with policer action (SRX Series Devices)**—When you upgrade your device to Junos OS Release 19.4R3-S1 or later, and the VPLS interface has an output filter with policer action applied to it, the VPLS interface does not pass the traffic. Because of this issue, the output bytes do not increment on that interface, and when you display details using the `show interfaces <interface-name> extensive | no-more` command output, the VPLS interface shows output bytes as 0. In Junos OS Release 22.3R1, the `show interfaces interface-name extensive | no-more` command output shows the correct details.
- **Tunnel MTU**— On SRX5000 line, the tunnel MTU is not displayed in the CLI output if the tunnel MTU is not configured.

Known Limitations

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

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

Chassis Clustering

- 10GbE DAC cable is not supported at CTL or FAB link at SRX4100 and SRX4200 chassis cluster setup. PR1636365
- In Z-mode configuration, sometimes the statistics of back-up session might not be correct on fail-over from primary to back-up. PR1667098

High Availability

- In SRX4100 and SRX4200 devices, there is a hardware limitation of Intel 82599 NIC where maximum of 128 unit case MAC addresses and MAC filters are supported. For MNHA switching mode, if you define more than 127 virtual MACs on same revenue or AE interface, the extra (those beyond 127) virtual MAC filters could not be programmed to the NIC, so you would see traffics (towards those vMACs) got silently dropped. PR1687262

Infrastructure

- When upgrading from Junos OS Release 21.2 and earlier to Junos OS Release 21.2 and later, validation and upgrade fails. Upgrading requires the use of the no-validate command. PR1568757

Platform and Infrastructure

- On SRX4600 device, the CPU may overrun while performing sanity check due to incompatibility issues between ukern scheduler and Linux driver which might lead to traffic loss. PR1641517

VPNs

- In some scenarios, the SRX5000 line of devices might show obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. PR1432925

Open Issues

IN THIS SECTION

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

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

Class of Service (CoS)

- The show interfaces queue command output not correctly displaying bps values for throughput higher than 4.25Gbps. PR1596172

Flow-Based and Packet-Based Processing

- For accelerated flows such as Express Path, the packet or byte counters in the session close log and show session output take into account only the values that accumulated while traversing the NP. PR1546430
- When you perform ISSU with security VRF-group configuration, the ISSU cannot be completed successfully. PR1661935

Interfaces and Chassis

- Traffic drop might be seen on irb interface on SRX1500 device for network control forwarding class when verifying DSCP classification based on single and multiple code-points. PR1611623

Platform and Infrastructure

- In macOS platforms when Juniper Secure Connect client connects successfully, the client is not getting minimized to tray icon and needs to be minimized manually.PR1525889
- With ssl-proxy configured along with web-proxy, the client session might not closed on the device even though proxy session ends gracefully. PR1580526
- HA active/passive mode on-box logging in logical systems and tenant systems, Intermittently Security log contents of binary log file in LSYS are not as expected. PR1587360
- SMTPS sessions are not getting identified when traffic is sent from IXIA (BPS) profile. PR1635929
- Firewall authentication with user firewall based RADIUS access has system logs missing the username and rule. PR1654842
- The show security firewall-authentication users identifier 1 and show security firewall-authentication users address 10.1.1.1 commands does not display user's group information. PR1659115
- The primary password for configuration encryption and FIPS mode should not be enabled together.PR1665506
- The show services user-identification authentication-table ip-address command is failing when auth entry boundary testing with auth entry containing maximum length group-name and resource-group-name is used. PR1665691

VPNs

- In some scenarios, the kmd process might generate core files when all VPNs are down. PR1336368

Resolved Issues

IN THIS SECTION

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

Chassis Clustering

- MSISDN prepended with additional digits in the logs. PR1646463
- Failover might not happen correctly in a chassis cluster when there is a hardware issue with the Central Point. PR1651501
- In the MNHA SRG scenario on the IPv6 switching mode, not using Virtual MAC as the source MAC address for G-NDP. PR1670309
- GTP control packets might be incorrectly dropped or passed if there is more than one APN IMSI filter configured. PR1673879

Flow-Based and Packet-Based Processing

- The traffic might get lost when using dedicated HA fabric link. PR1651836
- Performance degradation might be observed when Express Path and PME are both enabled. PR1652025
- The gre-performance-acceleration might cause VPLS traffic drop. PR1661409
- vSRX not processing fragmented packets. PR1668898

Interfaces and Chassis

- The redundant Ethernet1 interface down and DCD generates cores files on node1. PR1657021

Intrusion Detection and Prevention (IDP)

- The flowd process might generate core files when IDP policy rulebase changes. PR1657056

J-Web

- Significant performance improvements were made to J-Web in this release. PR1652676
- Various page errors have been corrected in J-Web. PR1658330

Platform and Infrastructure

- Syslog message %AUTH-3: warning: can't get client address: Bad file descriptor is displayed at J-Web login. PR1581209
- Juniper Secure Client traffic gets dropped during reaching JSC installed client from server behind gateway in TCP path finder enabled VPN gateway. PR1611003
- VPLS interface fails to forward traffic on SRX Series devices. PR1611400
- Execute RSI on SRX5000 line of devices with IOC2 card installed may trigger data plane failover. PR1617103
- Traffic might be dropped due to the TX queue memory leak on PCI interface. PR1618913
- The PKID process stops due to null pointer dereferencing during local certificate verification in some cases. PR1624844
- A major alarm DPDK Tx stuck issue of SRX4100 and SRX4200 devices. PR1626562
- The show commands to display DNS cache summary, display only DNS cache C2 entries and display only DNS cache benign entries are needed. PR1631002
- On Junos platforms kernel panic might be seen during the boot sequence. PR1638923

- The junos-ssl-term is not found in ssl-trace-new logs. PR1640075
- Traffic might be dropped due to the RX queue being full. PR1641793
- Observing Error usp_ipc_client_recv_:ipc_pipe_read() due to core file,when checking show security monitoring CLI command. PR1641995
- The flowd process might stop when back to back sigpack is updated at the time of stress traffic. PR1642383
- On Juniper Secure Connect the remote-access-juniper-std license not getting freed up while disconnect or reconnect after RG0 failover. PR1642653
- The IMAP or IMAPS email permitted counter is not incremented in AAMW email statistics. PR1646661
- The severity of AAMW and SMS control and submission channel alarms have been reduced from major to minor to avoid triggering a chassis cluster failover in the event of an upstream network issue. PR1648330
- Unable to get the firewall-authentication users details on node 1. PR1651129
- SMB file submissions to ATP cloud failed. PR1653098
- The control link might not come up during the reboot. PR1654838
- Certificate based VPN tunnel is not established. PR1655571
- The fxp0 interface might remain UP when the cable is disconnected. PR1656738
- When service-set is configured with syslog and SSL, mspmand process might generate core files and might cause traffic disruption. PR1657027
- Radius responses that take longer than 15 seconds can cause SRX Series devices to declare authentication failure. PR1658833
- The configuration might roll back after performing commit confirmed and then reboot. PR1659783
- Cache miss counter increments twice instead of one. PR1663678
- SRX alarming SMS control channel down without SMS feature configured. PR1666420
- Information about users groups is not displayed completely. PR1673125
- The flowd process might stop when AAMW encounters a memory leak PR1675722

Routing Policy and Firewall Filters

- The utility monitor security packet-drop now correctly reports policy-related drops for unified policy. PR1576150
- Security policy state may be invalid on SRX Series devices. PR1669386
- The rpd process might stop before software upgrade. PR1670998
- SRX stops refreshing the FQDNs used in the security policies and NAT. PR1680749

Routing Protocols

- Delay in BGP session establishment due to longer time for the listening task to be ready on all platforms running rpd process. PR1651211
- The BSR information might not be flooded over NG-MVPN. PR1664211

Unified Threat Management (UTM)

- UTM content filtering CLI is changing from seclog to log. PR1634580
- Modification of content filtering rule order after Junos OS release 21.4 would not have the desired effect. PR1653488

User Interface and Configuration

- The gethostbyname: hostname lookup failure is displayed during commit. PR1673176

VPNs

- Fragmented packets might drop when PMI is enabled. PR1624877
- Tunnel bringing up failed from strongswan when changing the configuration IKE in VR and observed the NO_PROPOSAL_CHOSEN notify error message. PR1627963

- Severity is unknown at some IPsec syslog messages. PR1629793
- Whenever SNMP get request is performed with multiple OIDs and a few OID requests are for invalid tunnels. PR1632932
- IPsec tunnel might stop processing traffic. PR1636458
- The IPsec tunnel through IPv6 might not establish after rebooting SRX Series devices. PR1653704
- The Juniper secure connect VPN users may face login issues intermittently. PR1655140
- The device enabled with FIPS mode and rebooted the system fails to boot. PR1655355
- Packets traversing through a policy-based VPN get dropped when PMI is enabled. PR1663364
- The IPsec tunnels may flap on SRX Series devices. PR1665332
- The control plane CPU utilization might reach 100% while KMD process stuck after core files generated on SRX345 device. PR1673391

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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

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

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

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

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

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 13: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Junos OS Release Notes for vMX

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for vMX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for vMX.

Junos Telemetry Interface

- **Support for VLAN sensors (ACX5448, ACX5448-M, ACX5448-D, and ACX710 routers, EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650,**

EX4650-48Y-VC and EX9208 switches, MX204, MX240, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2010, MX2020, PTX10008, and PTX10016 routers and vMX)—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports the data model **openconfig-vlan.yang** version 3.2.1, including sensor support to stream VLAN and MAC- limit operational states through telemetry.

[See Telemetry Sensor Explorer.]

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R1 for vMX.

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

Learn about the issues fixed in this release for vMX.

Upgrade Instructions

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

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

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

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

Junos OS Release Notes for vRR

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for vRR. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for vRR.

Junos Telemetry Interface

- **BGP policy sensor upgrade (ACX710, ACX5448, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10002, and vRR)**—Starting in Junos OS Release 22.3R1, Junos telemetry interface (JTI) supports data model **openconfig-bgp-policy.yang** version 6.0.2 (upgraded from version 4.0.1). JTI also supports new BGP policy sensors.

  [See Telemetry Sensor Explorer.]

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R1 for vRR.

Known Limitations

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

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

To learn more about common BGP or routing known limitations in Junos OS 22.3R1, see "Known Limitations" on page 88 for MX Series routers.

Open Issues

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

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

Resolved Issues

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

Junos OS Release Notes for vSRX

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R1 for vSRX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for vSRX.

High Availability

- **Multinode High Availability (SRX5400, SRX5600, and SRX5800 with SPC3, IOC3, SCB3, SCB4, and RE3; SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 22.3R1, we extend Multinode High Availability support to SRX4600, SRX4200, SRX4100, and SRX1500 devices and vSRX 3.0 instances. In this release, we support the following network deployment modes:

  - Layer 3 network
  - Default gateway
  - Hybrid network
  - Public cloud deployment (AWS)

  SRX Series devices with Multinode High Availability support firewall and advanced security services such as application security, Content Security, intrusion prevention system (IPS), firewall user authentication, NAT, and ALG. For the complete list of features supported with Multinode High Availability, see Feature Explorer.

  [See Multinode High Availability.]

- **PKI-based link encryption (SRX5400, SRX5600, and SRX5800 with SPC3, IOC3, SCB3, SCB4, and RE3; SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 22.3R1, we support PKI-based link encryption for interchassis links (ICLs) in Multinode High Availability. PKI provides a way of verifying the identity of a remote site by using a digital certificate.

  You can now generate and store node-specific PKI objects such as local keypairs, local certificates, and certificate-signing requests on both nodes. You can generate, view, and clear node-specific certificates using the CLI commands with the `node-local` option.

[See Multinode High Availability, request security pki node-local generate-key-pair, request security pki node-local generate-certificate-request, and show security pki node-local local-certificate.]

VPNs

- **Deprecated IPsec manual VPN configuration statement (SRX Series devices and vSRX instances that run the kmd process))**—Starting in Junos OS Release 22.3R1, we've deprecated the manual IPsec VPN (flow mode) configuration. Therefore, you cannot establish a manual IPsec security association through the [`edit security ipsec vpn` *`vpn-name`* `manual`] configuration hierarchy.

  [See manual (Security IPsec).]

What's Changed

IN THIS SECTION

Learn about what changed in this release for vSRX.

Platform and Infrastructure

- SRX Series devices does not drop session with server certificate chain more than 6.

Unified Threat Management (UTM)

- **Content filtering CLI updates (SRX Series and vSRX)**—We've the following updates to the content filtering CLI:

- Trimmed the list of file types supported for content filtering rule match criteria. Instead of uniquely representing different variants of a file type, now only one `file-type` string represents all variants. Hence, the `show security utm content-filtering statistics` output is also updated to align with the new file types available in the rule match criteria.
- Renamed the content filtering security logging option `seclog` to `log` to match with the Junos OS configuration standard.
- Rephrased the `reason` string associated with content filtering security log message.

[See show security utm content-filtering statistics, content-filtering (Security Feature Profile), and content-filtering (Security UTM Policy).]

VPNs

- **IKEv1 Tunnel establishment not allowed with HSM enabled (vSRX3.0)**—On vSRX 3.0, you can safeguard the private keys used by `pkid` and `iked` processes using Microsoft Azure Key Vault hardware security module (HSM) service.

  But, you cannot configure Internet Key Exchange version 1 (IKEv1) after enabling the HSM service. If you still try to configure IKEv1 when HSM is enabled, a warning message is displayed.

VPNs

- **Changes to IP address byte order (vSRX 3.0)**—In syslog messages for **KMD_VPN_DOWN_ALARM_USER** and **KMD_VPN_UP_ALARM_USER**, the IP address byte order now appears in the correct order as against the reverse byte order which was appearing in earlier releases.

Known Limitations

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

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

Open Issues

IN THIS SECTION

Learn about open issues in this release for vSRX.

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

Platform and Infrastructure

- With SSL proxy configured along with web proxy, the client session might not get closed on the device even though proxy session ends gracefully. PR1580526

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for vSRX.

Flow-Based and Packet-Based Processing

- The traffic in the power-mode still passthrough when the ingress logic interface is manually disabled. PR1604144
- Expected TCP sequences not found in ICMPv6 dump. PR1611202
- Maintain 1 to 2 minutes gap between two configuration commits in huge security policies case. PR1625531
- TCP-MSS override for GREoIPSec does not work. PR1630124
- vSRX not processing fragmented packets. PR1668898

J-Web

- Significant performance improvements were made to J-Web in this release. PR1652676
- Various page errors have been corrected in J-Web. PR1658330

Network Address Translation (NAT)

- Datapath process might stop resulting in total traffic and service failure. PR1645039

Platform and Infrastructure

- Tag "RT_FLOW_SESSION_XXX" is missing in stream mode. PR1565153
- The junos-ssl-term is not found in ssl-trace-new logs. PR1640075
- AMR first session traffic is not copying over multiple paths for IPv6 traffic over IPv6 IPsec tunnel mode. PR1643570
- Certificate based VPN tunnel is not established. PR1655571
- The crash files might be seen on SRX Series devices. PR1655808
- Cache miss counter increments twice instead of one. PR1663678

Routing Policy and Firewall Filters

- The utility monitor security packet-drop now correctly reports policy-related drops for unified policy. PR1576150

Subscriber Access Management

- Same set of ciphers used in all 3 cipher categories low or medium or strong. PR1646260

Unified Threat Management (UTM)

- UTM content filtering CLI is changing from seclog to log. PR1634580
- Modification of content filtering rule order after Junos OS release 21.4 would not have the desired effect. PR1653488
- The browser traffic might get blocked when matched to the content filtering rule with file-types 7z. PR1656266

VPNs

- IPsec tunnel might stop processing traffic. PR1636458
- The ipsec tunnel-events-statistics command output is not coming as expected while verifying IPv4 autovpn in P2MP mode using IKEv2 with DUT as spoke with latest DCB. PR1669110

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

You also can upgrade to Junos OS Release 22.3R1 for vSRX using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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

The following limitations apply:

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

  Check this using the following command:

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

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

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

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 22.3R1 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 Aug 25 14:15 /var/jail/tmp/alarmd.ts
       259.7K Aug 25 14:11 /var/log/hostlogs/vjunos0.log.1.gz
```

```
        494B Aug 25 14:15 /var/log/interactive-commands.0.gz
        20.4K Aug 25 14:15 /var/log/messages.0.gz
        27B Aug 25 14:15 /var/log/wtmp.0.gz
        27B Aug 25 14:14 /var/log/wtmp.1.gz
        3027B Aug 25 14:13 /var/tmp/BSD.var.dist
        0B Aug 25 14:14 /var/tmp/LOCK_FILE
        666B Aug 25 14:14 /var/tmp/appidd_trace_debug
        0B Aug 25 14:14 /var/tmp/eedebug_bin_file
        34B Aug 25 14:14 /var/tmp/gksdchk.log
        46B Aug 25 14:14 /var/tmp/kmdchk.log
        57B Aug 25 14:14 /var/tmp/krt_rpf_filter.txt
        42B Aug 25 14:13 /var/tmp/pfe_debug_commands
        0B Aug 25 14:14 /var/tmp/pkg_cleanup.log.err
        30B Aug 25 14:14 /var/tmp/policy_status
        0B Aug 25 14:14 /var/tmp/rtsdb/if-rtsdb
        Delete these files ? [yes,no] (no) yes
<
output omitted>
```

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

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 22.3R1 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-20.4-2022-08-08.0_RELEASE_22.3_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-
x86-64-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 22.3 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-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_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-22.3-2022-08-08.0_RELEASE_22.3_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-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_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-22.3-2022-08-08.0_RELEASE_22.3_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-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-linux.tgz completed
upgrade_platform: System need *REBOOT* to complete the upgrade
upgrade_platform: Run upgrade_platform with option -r | --rollback to rollback the upgrade
Host OS upgrade staged. Reboot the system to complete installation!
WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software rollback'
WARNING:     command as soon as this operation completes.
NOTICE: 'pending' set will be activated at next reboot...
Rebooting. Please wait ...
shutdown: [pid 13050]
Shutdown NOW!
*** FINAL System shutdown message from root@ ***
System going down IMMEDIATELY
Shutdown NOW!
System shutdown time has arrived\x07\x07
```

If no errors occur, Junos OS reboots automatically to complete the upgrade process. You have successfully upgraded to Junos OS Release 22.3R1 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 22.3-2022-08-08.0_RELEASE_22.3_THROTTLE Kernel 64-bit
JNPR-11.0-20171012.170745_fbsd-
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ # cli
root> show version
Model: vsrx
Junos: 22.3-2022-08-08.0_RELEASE_22.3_THROTTLE
JUNOS OS Kernel 64-bit  [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]
JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_ssd-builder_release_174_throttle]
```

Validating the OVA Image

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

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

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

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

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

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 14: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Licensing

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

The major components of the framework are:

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

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

Finding More Information

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

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

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

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

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

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

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

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

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

Requesting Technical Support

IN THIS SECTION

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/

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

17 January 2025—Revision 12, Junos OS Release 22.3R1.

20 July 2023—Revision 11, Junos OS Release 22.3R1.

23 February 2023—Revision 10, Junos OS Release 22.3R1.

02 February 2023—Revision 9, Junos OS Release 22.3R1.

24 January 2023—Revision 8, Junos OS Release 22.3R1.

16 December 2022—Revision 7, Junos OS Release 22.3R1.

09 December 2022—Revision 6, Junos OS Release 22.3R1.

24 November 2022—Revision 5, Junos OS Release 22.3R1.

10 November 2022—Revision 4, Junos OS Release 22.3R1.

20 October 2022—Revision 3, Junos OS Release 22.3R1.

04 October 2022—Revision 2, Junos OS Release 22.3R1.

16 September 2022—Revision 1, Junos OS Release 22.3R1.