

Release Notes

Published
2023-07-20

Junos® OS Release 21.3R2

Table of Contents

Introduction | 1

Junos OS Release Notes for ACX Series

What's New | 2

What's New in 21.3R2 | 2

What's New in 21.3R1 | 2

Hardware | 2

Junos Telemetry Interface | 3

Layer 2 VPN | 3

Routing Protocols | 3

Source Packet Routing in Networking (SPRING) or Segment Routing | 4

Additional Features | 4

What's Changed | 5

What's Changed in Release 21.3R2 | 5

What's Changed in Release 21.3R1 | 6

Known Limitations | 8

Open Issues | 9

Resolved Issues | 10

Resolved Issues: 21.3R2 | 11

Resolved Issues: 21.3R1 | 13

Documentation Updates | 16

Migration, Upgrade, and Downgrade Instructions | 16

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 16

Junos OS Release Notes for cSRX

What's New | 18

What's New in 21.3R2 | 18

| What's New in 21.3R1 | 18

What's Changed | 18

Known Limitations | 18

Open Issues | 19

Resolved Issues | 19

Documentation Updates | 19

Junos OS Release Notes for EX Series

What's New | 20

| What's New in 21.3R2 | 20

| What's New in 21.3R1 | 20

| Hardware | 20

| Application Identification (AppID) | 21

| Additional Features | 21

What's Changed | 21

| What's Changed in Release 21.3R2 | 21

| What's Changed in Release 21.3R1 | 22

Known Limitations | 25

Open Issues | 26

Resolved Issues | 28

| Resolved Issues: 21.3R2 | 28

| Resolved Issues: 21.3R1 | 32

Documentation Updates | 38

Migration, Upgrade, and Downgrade Instructions | 38

| Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life
Releases | 38

Junos OS Release Notes for JRR Series

What's New | 40

What's New in 21.3R2 | 40

What's New in 21.3R1 | 40

| Routing Protocols | 40

What's Changed | 41

| What's Changed in Release 21.3R2 | 41

Known Limitations | 41

Open Issues | 41

Resolved Issues | 42

| Resolved Issues: 21.3R2 | 42

| Resolved Issues: 21.3R1 | 42

Documentation Updates | 43

Migration, Upgrade, and Downgrade Instructions | 43

| Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life
Releases | 43

Junos OS Release Notes for Juniper Secure Connect

What's New | 45

What's New in 21.3R2 | 45

What's New in 21.3R1 | 45

| Additional Features | 45

What's Changed | 46

Known Limitations | 46

Open Issues | 46

Resolved Issues | 46

Documentation Updates | 46

Junos OS Release Notes for Junos Fusion for Enterprise

What's New | 47

What's Changed | 47

Known Limitations | 48

Open Issues | 48

Resolved Issues | 48

Resolved Issues: 21.3R2 | 48

Resolved Issues: 21.3R1 | 49

Documentation Updates | 49

Migration, Upgrade, and Downgrade Instructions | 49

Junos OS Release Notes for Junos Fusion for Provider Edge

What's New | 56

What's Changed | 56

Known Limitations | 56

Open Issues | 56

Resolved Issues | 57

Resolved Issues: 21.3R2 | 57

Documentation Updates | 57

Migration, Upgrade, and Downgrade Instructions | 58

Junos OS Release Notes for MX Series

What's New | 68

What's New in 21.3R2 | 68

What's New in 21.3R1 | 68

Hardware | 69

Chassis | 69

IP Tunneling | 69

IPv6 | 70

Junos Telemetry Interface | 70

Layer 2 VPN | 71

MPLS | 71

Network Address Translation (NAT) | 72

Platform and Infrastructure	72
Routing Options	72
Routing Protocols	73
Source Packet Routing in Networking (SPRING) or Segment Routing	74
Subscriber Management and Services	75
System Management	76
VPNs	76
Additional Features	77

What's Changed | 78

What's Changed in Release 21.3R2	78
What's Changed in Release 21.3R1	80

Known Limitations | 83

Open Issues | 85

Resolved Issues | 96

Resolved Issues: 21.3R2	97
Resolved Issues: 21.3R1	113

Documentation Updates | 136

Migration, Upgrade, and Downgrade Instructions | 136

Junos OS Release Notes for NFX Series

What's New | 142

What's New in 21.3R2	142
What's New in 21.3R1	142
Application Identification (AppID)	142

What's Changed | 143

Known Limitations | 143

Open Issues | 144

Resolved Issues | 145

Resolved Issues: 21.3R2	145
-------------------------	-----

Resolved Issues: 21.3R1 | 145

Documentation Updates | 147

Migration, Upgrade, and Downgrade Instructions | 147

Junos OS Release Notes for PTX Series

What's New | 149

What's New in 21.3R2 | 150

What's New in 21.3R1 | 150

IP Tunneling | 150

Junos Telemetry Interface | 150

MPLS | 151

Routing Policy and Firewall Filters | 151

Routing Protocols | 151

Source Packet Routing in Networking (SPRING) or Segment Routing | 152

Services Applications | 152

Additional Features | 153

What's Changed | 153

What's Changed in Release 21.3R2 | 154

What's Changed in Release 21.3R1 | 155

Known Limitations | 159

Open Issues | 160

Resolved Issues | 162

Resolved Issues: 21.3R2 | 162

Resolved Issues: 21.3R1 | 164

Documentation Updates | 168

Migration, Upgrade, and Downgrade Instructions | 168

Junos OS Release Notes for QFX Series

What's New | 173

What's New in 21.3R2 | 174

What's New in 21.3R1 | 174

- Hardware | 174
- EVPN | 175
- IP Tunneling | 176
- Routing Policy and Firewall Filters | 176
- Routing Protocols | 176
- Additional Features | 177

What's Changed | 177

- What's Changed in Release 21.3R2 | 178
- What's Changed in Release 21.3R1 | 178

Known Limitations | 182**Open Issues | 184****Resolved Issues | 189**

- Resolved Issues: 21.3R2 | 189
- Resolved Issues: 21.3R1 | 195

Documentation Updates | 202**Migration, Upgrade, and Downgrade Instructions | 202****Junos OS Release Notes for SRX Series****What's New | 217****What's New in 21.3R2 | 217****What's New in 21.3R1 | 217**

- Application Identification (AppID) | 218
- Flow-Based and Packet-Based Processing | 219
- Intrusion Detection and Prevention | 219
- J-Web | 219
- Juniper Advanced Threat Prevention Cloud (ATP Cloud) | 221
- Network Management and Monitoring | 221
- VPNs | 222
- Additional Features | 222

What's Changed | 223

What's Changed in Release 21.3R2 | 223

What's Changed in Release 21.3R1 | 224

Known Limitations | 226

Open Issues | 227

Resolved Issues | 230

Resolved Issues: 21.3R2 | 231

Resolved Issues: 21.3R1 | 234

Documentation Updates | 241

Migration, Upgrade, and Downgrade Instructions | 241

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 241

Junos OS Release Notes for vMX

What's New | 243

What's New | 243

What's Changed | 243

What's Changed in Release 21.3R2 | 244

What's Changed in Release 21.3R1 | 244

Known Limitations | 245

Open Issues | 245

Resolved Issues | 245

Resolved Issues: 21.3R2 | 246

Resolved Issues: 21.3R1 | 246

Documentation Updates | 247

Upgrade Instructions | 247

Junos OS Release Notes for vRR

What's New | 248

What's New in 21.3R2 | 248

What's New in 21.3R1 | 248

| Application Identification (AppID) | 248

What's Changed | 249

| What's Changed in Release 21.3R2 | 249

Known Limitations | 249

Open Issues | 249

Resolved Issues | 250

| Resolved Issues: 21.3R2 | 250

Documentation Updates | 250

Junos OS Release Notes for vSRX

What's New | 251

| What's New in 21.3R2 | 251

| What's New in 21.3R2 | 252

What's Changed | 252

| What's Changed in Release 21.3R2 | 252

| What's Changed in Release 21.3R1 | 253

Known Limitations | 254

Open Issues | 254

Resolved Issues | 256

| Resolved Issues: 21.3R2 | 256

| Resolved Issues: 21.3R1 | 258

Documentation Updates | 260

Migration, Upgrade, and Downgrade Instructions | 260

| Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life
Releases | 266

Licensing | 267

Finding More Information | 268

Documentation Feedback | 269

Requesting Technical Support | 269

Revision History | 271

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 21.3R1 for the ACX Series, Containerized Routing Protocol Process (cRPD), cSRX Container Firewall (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, virtual MX Series router (vMX), Virtual Route Reflector (vRR), and vSRX Virtual Firewall (vSRX). They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Junos OS Release Notes for ACX Series

IN THIS SECTION

- [What's New | 2](#)
- [What's Changed | 5](#)
- [Known Limitations | 8](#)
- [Open Issues | 9](#)
- [Resolved Issues | 10](#)
- [Documentation Updates | 16](#)
- [Migration, Upgrade, and Downgrade Instructions | 16](#)

These release notes accompany Junos OS Release 21.3R2 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

- [What's New in 21.3R2](#) | 2
- [What's New in 21.3R1](#) | 2

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

What's New in 21.3R2

There are no new features or enhancements to existing features in Junos OS Release 21.3R2 for the ACX Series.

What's New in 21.3R1

IN THIS SECTION

- [Hardware](#) | 2
- [Junos Telemetry Interface](#) | 3
- [Layer 2 VPN](#) | 3
- [Routing Protocols](#) | 3
- [Source Packet Routing in Networking \(SPRING\) or Segment Routing](#) | 4
- [Additional Features](#) | 4

Hardware

- **Support for QSFP-100G-FR and QSFP-100G-LR transceivers (ACX5448, ACX5448-M, and ACX5448-D)**—Starting in Junos OS Release 21.3R1, the ACX5448, ACX5448-M, and ACX5448-D switches support the QSFP-100G-FR and QSFP-100G-LR transceivers.

[See [Hardware Compatibility Tool](#).]

- **Support for passive optical network (PON) controller integration with 10G OLT SFP+ transceiver (ACX5448, ACX5448-M, and ACX5448-D routers)**—Starting in Junos OS Release 21.3R1, the ACX5400 line of routers support the integration of the PON controller with Juniper Networks' 10GbE optical line terminal (OLT) SFP+ transceiver. This transceiver plugs into the 10GbE ports and instantaneously enables 10GbE symmetrical PON access on the router. Because the ACX5400 line of routers function as the OLT, the use of this transceiver eliminates the need for additional hardware. The following softwares are supported for Juniper's Unified PON in Junos OS Release 21.3R1:

- PON Controller version R2.0.4
- MicroClimate Management System PON Manager version R2.1.2
- MicroClimate Management System NETCONF Server version R2.1.1

[See [Juniper's Unified PON - Integrated PON Controller on ACX5400 Line of Routers](#) and [Hardware Compatibility Tool](#).]

Junos Telemetry Interface

- **Telemetry stream path resolution by MPLS and RSVP interfaces (ACX710, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5448, ACX4558-D, ACX5448-M, MX150, MX204, MX340, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, vMX, PTX1000, PTX3000, PTX5000, PTX10002-60C, and PTX10008)**—Starting in Junos OS Release 21.3R1, you can choose to stream telemetry statistics only for MPLS and RSVP-enabled interfaces. Use the resource path `/network-instances/network-instance/mpls/signaling-protocols/rsvp-te/interface-attributes/interface/admin-status`.

[See [Configuring a Junos Telemetry Interface Sensor \(CLI Procedure\)](#) and [Telemetry Sensor Explorer](#).]

Layer 2 VPN

- **No-local switching on VPLS (ACX710 and ACX5448)**—Starting in Junos OS Release 21.3R1, you can configure the ACX710 and the ACX5448 routers to support no local switching. When the no local switching feature is enabled, packets from CE devices will only be forwarded to PE devices and core-facing interfaces. Packet will not be forwarded to other CE devices that are part of the VPLS routing instance domain. To include the no-local-switching statement at the `[edit routing-instances instance-name]` hierarchy level.

[See [no-local-switching](#) .]

Routing Protocols

- **Check for AS match in BGP policy AS paths without using regular expressions (ACX5048, ACX5096, ACX5448, MX240, MX480, MX960, MX2008, MX10016, vMX, PTX1000, PTX5000, PTX10001, PTX10002, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, and QFX10016)**—Starting in

Junos OS Release 21.3R1, you can configure BGP policies to check for an autonomous system (AS) match in an AS path without using regular expressions. The BGP policy compares the AS to an AS-list or AS-list-group and returns true if it finds a match. You can configure the BGP policy to check for a matching origin, neighbor, or transit AS. This feature provides a faster alternative to match origin, transit, and peer AS numbers than using a regular expression.

Configure this feature using the `as-path-neighbors`, `as-path-origins`, or `as-path-transits` option at the `[edit policy-options policy-statement policy-name from]` hierarchy level. For each type of match, use `(as-list | as-list-group) as-list-name/as-list-group-name` to specify the list or group of AS paths to compare the match to. Configure the AS list or AS group at the `[edit policy-options]` hierarchy level.

[See [policy-options](#) and [policy-statement](#).]

- **Maximum reference bandwidth increased to 4 TB for IGP protocols (ACX710, ACX5448, MX960, MX2020, MX10003, PTX5000, and PTX1000)**—Starting in Junos OS Release 21.3R1, we've increased the maximum reference bandwidth for IS-IS and OSPF IGP protocols from 1 Tbps to 4 Tbps. The default bandwidth is 100 Mbps. You can increase the reference bandwidth to adjust the path metrics, which you use to determine the preferred path in case of multiple equal-cost routes to a destination.

To configure the reference bandwidth, use the `reference-bandwidth reference-bandwidth` statement at the `[edit protocols isis]` hierarchy level or the `[edit protocols (ospf | ospf3)]` hierarchy level.

[See [reference-bandwidth \(Protocols IS-IS\)](#) and [reference-bandwidth \(Protocols OSPF\)](#).]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Support for Application Specific Link Attributes (ASLA) for flexible algorithms (ACX710, MX204, MX240, MX480, MX960, MX10003, MX 10008, MX10016, MX2008, MX2010, MX2020, PTX1000, PTX5000, PTX10002, PTX10008, PTX10016, VMX)**: IS-IS supports advertising different `te-metric` and `admin-groups` for RSVP and flexible algorithm on the same link using flexible-algorithm specific ASLA as defined in RFC 8919.

[See [strict-asla-based-flex-algorithm](https://www.juniper.net/documentation/us/en/software/junos/is-is/topics/ref/statement/protocols-isis-source-packet-routing-strict-asla-based-flex-algorithm.html)<https://www.juniper.net/documentation/us/en/software/junos/is-is/topics/ref/statement/protocols-isis-source-packet-routing-strict-asla-based-flex-algorithm.html>.]

Additional Features

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

- **HQoS support is available on AE and MC-LAG (ACX5448)**
[See [Understanding Hierarchical CoS for Subscriber Interfaces](#).]
- **SPRING support for SR-TE (ACX 710 and ACX 5448):**

- Segment routing policy to steer labeled or IP traffic at ingress routers.
- Segment routing paths for a non-colored static label-switched path (LSP).
- Color-based traffic steering of Layer 2 and Layer 3 VPN services.
[See [Segment Routing Traffic Engineering at BGP Ingress Peer Overview](#)]
- **TWAMP Light IPv6 addressing support** (ACX710, ACX2000, ACX2100, ACX5448, MX5, MX10, MX40, MX80, MX104, MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10008, MX10016, vMX, PTX1000, and PTX5000)
[See [Understand Two-Way Active Measurement Protocol on Routers.](#)]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.3R2](#) | 5
- [What's Changed in Release 21.3R1](#) | 6

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

What's Changed in Release 21.3R2

IN THIS SECTION

- [Network Management and Monitoring](#) | 5
- [Routing Protocols](#) | 6

Network Management and Monitoring

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

- When you deactivate the entire [edit system configuration-database ephemeral] hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
- When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the delete-ephemeral-default statement in conjunction with the ignore-ephemeral-default statement at the [edit system configuration-database ephemeral] hierarchy level.

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

Routing Protocols

- To achieve consistency among resource paths, the resource path `/mpls/signalling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counterip-addr='address'/state/countersname='name'/out-pkts/` is changed to `/mpls/signaling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counterip-addr='address'/state/countersname='name'/`. The leaf `out-pkts` is removed from the end of the path, and `signalling` is changed to `signaling` (with one "l").

What's Changed in Release 21.3R1

IN THIS SECTION

- [EVPN | 6](#)
- [General Routing | 7](#)
- [Junos XML API and Scripting | 7](#)
- [Layer 2 Ethernet Services | 7](#)
- [Network Management and Monitoring | 8](#)

EVPN

- **Support for displaying SVLBNH information**—You can now view shared VXLAN load balancing next hop (SVLBNH) information when you display the VXLAN tunnel endpoint information for a specified ESI and routing instance by using the `show ethernet-switching vxlan-tunnel-end-point esi esi-identifier esi-identifier instance instance svlbh` command.

General Routing

- **Enhancement to the `show chassis pic` command**—You can now view additional information about the optics when you run the `show chassis pic` command. The output now displays the following additional field: MSA Version: Multi-source Agreements (MSA) version that the specified optics is compliant to. Values supported are: SFP+/SFP28 &-8212; SFF-8472 (versions 9.3 - 12.3), QSFP+/QSFP28 &-8212; SFF 8363 (versions 1.3 - 2.10), and QSFP-DD &-8212; CMIS 3.0, 4.0, 5.0. Previously, the `show chassis pic` command did not display this additional field.

[See [show chassis pic](#).]

- **Enhancement to the `show interfaces (Aggregated Ethernet) command`**—You can now view additional information about the MAC statistics when you run the `show interfaces extensive ae` command. The output now displays the following additional field: MAC statistics: Receive Transmit Broadcast packets 0 0 Multicast packets 0 0. Previously, the `show interfaces extensive ae` command did not display this additional field.

[See [show chassis pic](#).]

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS](#).]

Layer 2 Ethernet Services

- **Link selection support for DHCP**—We have introduced the `link-selection` statement at the `[edit forwarding-options dhcp-relay relay-option-82]` hierarchy level, which allows DHCP relay to add suboption 5 to option 82. Suboption 5 allows DHCP proxy clients and relay agents to request an IP address for a specific subnet from a specific IP address range and scope. Prior to this release, the DHCP relay dropped packets during the renewal DHCP process and the DHCP server used the leaf's address as a destination to acknowledge the DHCP renewal message.

[See [relay-option-82](#).]

Network Management and Monitoring

- **Changes in contextEngineID for SNMPv3 INFORMS (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Now the contextEngineID of SNMPv3 INFORMS is set to the local engine-id of Junos devices. In earlier releases, the contextEngineID of SNMPv3 INFORMS was set to remote engine-id.

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

Known Limitations

IN THIS SECTION

- [General Routing | 8](#)
- [Infrastructure | 9](#)

Learn about known limitations in Junos OS Release 21.3R2 for ACX Series routers.

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

General Routing

- The `ping` command on an ACX Series device might display variable latency values. This is expected for the host-generated ICMP traffic due to the design of the Packet Forwarding Engine queue polling the packets from ASIC. [PR1380145](#)
- On ACX710 routers running Junos OS Release 21.2R1 and later, the kernel might crash generating the `g_vfs_done()` logs. [PR1608852](#)

Infrastructure

- When you upgrade software from Junos OS Release 21.1 or earlier to Junos OS Release 21.2R1 or later, the image validation fails. You must use the no-validate options. For example, request system software add no-validate <image name>. [PR1568757](#)

Open Issues

IN THIS SECTION

- [General Routing | 9](#)
- [Platform and Infrastructure | 10](#)

Learn about open issues in Junos OS Release 21.3R2 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

- In a race condition, if a BGP route gets resolved over the same prefix protocol next hop in a routing table that has routes of the prefix from different routing protocols and when the routes flaps (initially the routes were in the Down state and then in the Up state), the BGP route gets re-resolved and the rpd process might crash. [PR1458595](#)
- On ACX710 routers, if you plug in the console cable, activate the terminal connection, and send characters to the interface, the system boot might be interrupted and the router boot gets stalled at the uboot# prompt. [PR1513553](#)
- Due to the BRCM KBP issue, route lookup might fail. [PR1533513](#)

- On ACX5448 routers, the following error message gets generated after you commit a class of service scheduler configuration:

```
LIBCOS_COS_TVP_FC_INFO_NOT_FOUND: Forwarding-class information not specified
```

[PR1579009](#)

- When you configure the multihop BFD sessions, the delegated BFD sessions do not come up. [PR1633395](#)
- IGMP snooping configuration drops the Layer 2 VPN multicast traffic. [PR1628600](#)
- On ACX5448 routers, if you configure hierarchical-scheduler for an interface during interface flap or configuration change, some of the Packet Forwarding Engine buffers might become out of synchronization, which might cause packets drops even without congestion. [PR1603622](#)
- USB installation requires a keypress before reboot to enable the removal of the USB device before system gets restarted. Failing to remove the USB stick causes installation to start again. You must use the keypress after installation. [PR1640143](#)

Platform and Infrastructure

- The vmxt_lnx process generates core file at topo_get_link jnh_features_get_jnh jnh_stream_attach. [PR1638166](#)

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.3R2 | [11](#)
- Resolved Issues: 21.3R1 | [13](#)

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

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

Resolved Issues: 21.3R2

IN THIS SECTION

- [General Routing | 11](#)

General Routing

- On ACX5448 routers, when you have both the CFM and BFD configured on the system, the BFD session status goes in to the Init state after the system reboots. [PR1552235](#)
- On ACX710 routers, PTP might get stuck and does not function properly in certain condition. [PR1587990](#)
- Specific packets over VXLAN causes FPC memory leakage and ultimately resets the Packet Forwarding Engine. [PR1602407](#)
- On ACX5448 routers, CFM does not go into the Ok state after the router reboots. [PR1602489](#)
- On ACX5448 and ACX710 routers, running the DHCP relay does not process the packets arriving over MPLS. [PR1605854](#)
- On ACX5096 routers, the output of the pps traffic is displayed on the deactivated interfaces. [PR1608827](#)
- On ACX710 routers running Junos OS Release 21.2R1 and later might cause kernel to crash. [PR1608852](#)
- On ACX5448 and ACX710 routers, traffic towards the CE devices through the default route might be dropped in VRF. [PR1611651](#)
- On ACX5448 routers, the following error message gets generated while overriding the baseline configuration from the profile configuration:

```
fpc0 DNX_NH::dnx_nh_unilist_install_multipath(),1053: Error creating ecmp egress object:
unilist nh 2097463, intf cnt 0 (-4:Invalid parameter)
```

[PR1612026](#)

- The routing protocol engine CPU gets stuck at 100 percent. [PR1612387](#)

- On ACX5448 routers with rates above 4 GB, there might be mismatches in the statistics between the physical and logical interfaces. [PR1614550](#)
- Host-outbound-traffic might be placed in the incorrect queue. [PR1619174](#)
- Traffic might get equally load-balanced irrespective of the scheduler configuration. [PR1620137](#)
- In IGMP, there might be 6 to 8 seconds delay when the receiver switches in between the groups. [PR1620685](#)
- Traffic forwarding to one of the the single homed PE devices or routers does not occur after the VLAN-ID gets changed under the routing instance. [PR1621036](#)
- On ACX5448 and ACX710 routers with Layer 3 VPN scenarios, after multiple core link or protocol flaps, error messages might get generated. [PR1621425](#)
- SNMP interface reports temperature instead of the RX alarms. [PR1621894](#)
- On ACX5448 routers, the smartd configurations do not get applied. [PR1623359](#)
- On ACX5448 routers, the EXP rewrite does not work in a Layer 3 VPN scenario when you configure the mf filter. [PR1623922](#)
- On ACX5000 routers, the local fault and remote fault signaling do not get logged on the `/var/log/messages` file. [PR1624761](#)
- On ACX5048 routers, the filters that reports the TCAM errors do not get installed in the hardware after upgrading from Junos OS Release 17.4R2-S8 to 20.4R3. [PR1630280](#)
- DHCP clients might not come online in the IRB with VLAN or EVPN scenario. [PR1633778](#)
- On ACX5448 routers, incorrect PEM overload alarm threshold gets displayed. [PR1636222](#)
- ZTP does not work on the et-x interfaces. [PR1601798](#)
- On ACX5448 and ACX710 routers, MPLS traffic might not be forwarded properly after reboot. [PR1605591](#)
- ACX Series routers running DHCP might not process packets arriving over IRB or MPLS. [PR1607201](#)
- Packet fragmentation might be seen when you configure MTU for the logical interface. [PR1614449](#)
- When you configure `vlan-id-range` or `list` for the aggregated Ethernet interface of `I2ckt`, traffic forwarding occurs for the first VLAN. [PR1616147](#)
- Traffic might not be forwarded after failover in the Layer 2 circuit hot standby mode. [PR1616892](#)
- On ACX710 and ACX5448 routers, the Packet Forwarding Engine daemon crashes if you disable the standby interface in the Layer 2 Circuit Pseudowire redundancy scenario. [PR1617287](#)

- Unicast packet loss might be observed due to the control-word configuration. [PR1626058](#)
- VPLS traffic loss might be observed post route flap. [PR1626267](#)
- ACX710 routers running G.8275.2 becomes nonresponsive at the PTP Acquiring state if the connection is through some timing unaware nodes. [PR1632761](#)
- The storm-control rate-limit might not work with VPLS policer under logical child interface. [PR1633427](#)
- ISIS last transition time never increments [PR1634747](#)
- The IS-IS last transition time never increments. [PR1634747](#)
- On ACX5448 and ACX710 routers, the Layer 3 interface creation might fail. [PR1638581](#)
- The Packet Forwarding Engine might crash after the device reboots or the Packet Forwarding Engine restarts. [PR1626503](#)
- On ACX5048 and ACX5096 routers, speed 10m configuration error occurs. [PR1633226](#)
- On ACX5448 routers with ESI configured, locally switched traffic might be dropped. [PR1638386](#)

Resolved Issues: 21.3R1

IN THIS SECTION

- [General Routing | 13](#)
- [Infrastructure | 15](#)
- [Platform and Infrastructure | 15](#)
- [Routing Protocols | 15](#)

General Routing

- On ACX5448 routers, the two-way time error and CTE for 1 PPS do not meet the class A metrics. [PR1535434](#)
- The DNX router fails to program Mcast route in BCM when the route has pime interface as outgoing interface. [PR1560914](#)
- Inline BFD stays down with the ISIS/Static clients. [PR1561590](#)

- On ACX5048 routers, the traffic-input-pps does not increment in the vlantagged_flexible traffic. [PR1569763](#)
- The l2circuit and CFM sessions might go down when you configure the asynchronous-notification. [PR1572722](#)
- ARP traffic that exceeds the policer limit does not get discarded. [PR1573956](#)
- On ACX5448 and ACX710 routers, 802.1P rewrite might not work. [PR1574601](#)
- Packets might get tagged with the default VLAN-ID and dropped at the peer in the Layer 2 circuits local switching scenario. [PR1574623](#)
- On ACX5448 routers, the packet buffer allocation error message appears when we scale the CFM sessions with the SLA iterator. [PR1574754](#)
- RLFA does not takes effect due to the service label wrongly added. [PR1577460](#)
- On ACX5448 routers, asynchronous-notification for 1G interface fails. [PR1580700](#)
- There might be a traffic drop between customer edge and provider edge devices in case of the ARP resolution failure. [PR1580782](#)
- The rpd process might get stuck due to the race condition. [PR1582226](#)
- On ACX710 routers, the jnpr-clock-recovery.log log file size appears to be small and archives rotates quickly. [PR1582350](#)
- On ACX710 routers, verifying the output of the channelized interface check with snmp mib get ifHighSpeed causes unexpected results. [PR1583995](#)
- On ACX5448 routers, IPv4 traffic loss with packet size more than 1410 occurs. [PR1584509](#)
- On ACX5448 routers, detection time shows the default value (6.000) along with the following error message instead of the configured value for single hop BFD.

```
ACX_ASIC_PROGRAMMING_ERROR
```

[PR1585382](#)

- On ACX710 routers, PTP might become nonresponsive and not function properly in certain condition. [PR1587990](#)
- On ACX710 and ACX5448 routers, DHCPv4 might not work. [PR1589135](#)
- On ACX710 and ACX5400 routers, traffic might get forwarded through the member links in the Down state after you add the new member links to the aggregated Ethernet interface. [PR1589168](#)

- On ACX710 and ACX5448 routers that runs DHCP relay does not process the packets arriving over MPLS with an explicit null label. [PR1590225](#)
- Traffic does not pass through the l2circuit interface when you configure the vlan-id-range. [PR1590969](#)
- On ACX5448 routers, high DMR out of sequence with iterator configuration occurs. [PR1596050](#)
- On ACX710 routers, the l2ald process generates core file at l2ald_event_process_list_id, l2ald_event_proc_all_lists, l2ald_event_periodic () at ../../../../src/junos/usr/sbin/l2ald/l2ald_event.c:757. [PR1596908](#)
- On ACX5448 and ACX710 routers, traffic drop occurs in the EVPN VPWS flexible cross connection. [PR1598074](#)
- On ACX5448 and ACX710 routers, traffic loss might be observed if drop-profiles is modified. [PR1598595](#)
- On ACX710 routers, rpf-check-bytes and rpf-check-packets counter does not get updated properly to the flat file as expected. [PR1600513](#)
- On ACX5448 routers, FPC might restart when you execute the show firewall command. [PR1605288](#)
- DHCP relay does not work in the routing-instance. [PR1605854](#)
- On the ACX5448 and ACX710 routers, the MACsec traffic over the Layer 2 circuit might not work. [PR1603534](#)
- On the ACX1000, ACX1100, ACX2000, ACX2100, and ACX4000 routers, the FEB (Forwarding Engine Board) might crash. [PR1606424](#)
- On the ACX710 and ACX5448 routers, the DHCP packets might not be relayed. [PR1608125](#)

Infrastructure

- The vme/me0 management interface cannot process any incoming packets. [PR1552952](#)

Platform and Infrastructure

- Upon receipt of the specific sequences of the genuine packets destined to the device, the kernel crashes and restarts. [PR1557881](#)

Routing Protocols

- The BGP session that carries the VPNv4 prefix with IPv6 next-hop might be dropped. [PR1580578](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R2 documentation for ACX Series.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 16

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 [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 cSRX

IN THIS SECTION

- [What's New | 18](#)
- [What's Changed | 18](#)
- [Known Limitations | 18](#)
- [Open Issues | 19](#)
- [Resolved Issues | 19](#)
- [Documentation Updates | 19](#)

These release notes accompany Junos OS Release 21.3R2 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

IN THIS SECTION

- [What's New in 21.3R2](#) | 18
- [What's New in 21.3R1](#) | 18

Learn about new features introduced in this release for cSRX.

What's New in 21.3R2

There are no new features or enhancements to existing features in Junos OS Release 21.3R2 for cSRX.

What's New in 21.3R1

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

What's Changed

There are no changes in behavior and syntax in Junos OS Releases 21.3R1, 21.3R2, and 21.3R3 for cSRX.

Known Limitations

There are no known limitations in hardware and software in Junos OS 21.3R2 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 and software in Junos OS Release 21.3R2 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

Learn about the issues fixed 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.

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R2 documentation for cSRX.

Junos OS Release Notes for EX Series

IN THIS SECTION

- [What's New | 20](#)
- [What's Changed | 21](#)
- [Known Limitations | 25](#)
- [Open Issues | 26](#)
- [Resolved Issues | 28](#)
- [Documentation Updates | 38](#)
- [Migration, Upgrade, and Downgrade Instructions | 38](#)

These release notes accompany Junos OS Release 21.3R2 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

- [What's New in 21.3R2](#) | 20
- [What's New in 21.3R1](#) | 20

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

What's New in 21.3R2

There are no new features or enhancements to existing features in Junos OS Release 21.3R2 for the EX Series switches.

What's New in 21.3R1

IN THIS SECTION

- [Hardware](#) | 20
- [Application Identification \(AppID\)](#) | 21
- [Additional Features](#) | 21

Hardware

- **Support for transceivers (EX4600 and EX4300-MP)**—Starting in Junos OS Release 21.3R1, the EX4600, EX4300 and EX4300-MP switches support these transceivers:
 - EX-SFP-10GE-LRM (EX4600 switches)

- JNP-QSFP-100G-PSM4 (EX4300-MP)
- JNP-QSFPP-40G-BXSR (EX4300-MP)
- JNP-QSFP-100G-BXSR (EX4300-MP)

[See [Hardware Compatibility Tool](#).]

Application Identification (AppID)

Additional Features

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

- **Precision Time Protocol (PTP) transparent clock** (EX4400-24MP, EX4400-24P, and EX4400-48MP)

[See [Understanding Transparent Clocks in Precision Time Protocol](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.3R2](#) | 21
- [What's Changed in Release 21.3R1](#) | 22

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

What's Changed in Release 21.3R2

IN THIS SECTION

- [Network Management and Monitoring](#) | 22
- [Routing Protocols](#) | 22
- [User Interface and Configuration](#) | 22

Network Management and Monitoring

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
 - When you deactivate the entire [edit system configuration-database ephemeral] hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
 - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
 - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the delete-ephemeral-default statement in conjunction with the ignore-ephemeral-default statement at the [edit system configuration-database ephemeral] hierarchy level.

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

Routing Protocols

- To achieve consistency among resource paths, the resource path `/mpls/signalling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counterip-addr='address'/state/countersname='name'/out-pkts/` is changed to `/mpls/signaling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counterip-addr='address'/state/countersname='name'/`. The leaf `out-pkts` is removed from the end of the path, and `signalling` is changed to `signaling` (with one "l").

User Interface and Configuration

- When you configure `max-cli-sessions` at the [edit system] hierarchy level, it restricts the maximum number of CLI sessions that can coexist at any time. Once the maximum-cli-sessions number is reached, new CLI access is denied. The users who are configured to get the CLI upon login, are also denied new login.

What's Changed in Release 21.3R1

IN THIS SECTION

- [General Routing | 23](#)
- [Junos XML API and Scripting | 23](#)

- [Interfaces and Chassis | 24](#)
- [Network Management and Monitoring | 24](#)
- [Platform and Infrastructure | 24](#)

General Routing

- [PR 1580601 -->](#)

Commit checks against incorrect configuration of SLC values (MX2020 and MX2010)—We have introduced commit checks against incorrect configuration of sub line cards (SLCs). While configuring SLCs, if you specify any incorrect values (for example, unsupported Packet Forwarding Engine ranges, CPU cores, or DRAM values), the configuration commit fails with an appropriate message to indicate the error.

[See [Configuring Sub Line Cards and Assigning Them to GNFs.](#)]

- **Enhancement to the show chassis pic command (Junos|Evo)**— You can now view additional information about the optics when you run the `show chassis pic` command. The output now displays the following additional field: MSA Version: Multi-source Agreements (MSA) version that the specified optics is compliant to. Values supported are: SFP+/SFP28 — SFF-8472 (versions 9.3 - 12.3), QSFP+/QSFP28 — SFF 8363 (versions 1.3 - 2.10), and QSFP-DD — CMIS 3.0, 4.0, 5.0. Previously, the `show chassis pic` command did not display this additional field.

[See [show chassis pic.](#)]

- **Juniper Agile Licensing (EX2300-VC, EX3400-VC, EX4300-VC, EX4400-24MP, EX4400-48MP, PTX10003, PTX10016, QFX5130-32CD, QFX5110-32Q, QFX5110-48S, QFX5120-48T, QFX5210-64C, QFX5200, and QFX5220)**—Starting from this release onwards, the Juniper Agile License Manager is deprecated. You can use the Juniper Agile Licensing Portal to activate, install, manage, and monitor licenses on Juniper Networks devices.

[See [Juniper Agile Licensing Guide.](#)]

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS.](#)]

Interfaces and Chassis

- When configuring multiple flexible tunnel interface (FTI) tunnels, the source and destination address pair needs to be unique only among the FTI tunnels of the same tunnel encapsulation type. Prior to this PR, the source and destination address pair had to be unique among all the FTI tunnels regardless of the tunnel encapsulation type.

Network Management and Monitoring

- **Chef and Puppet support removed (EX4400)**—Starting in Junos OS Release 21.3R1, EX4400 switches are migrated to FreeBSD 12.x based Junos OS. FreeBSD 12.x based Junos OS does not support installing existing Chef or Puppet packages.
- **Enhancement to the snmp mib walk command (PTX Series, QFX Series, EX Series, MX Series, SRX Series)**— The `ipv6IfOperStatus` field displays the current operational state of the interface. The `noIfIdentifier(3)` state indicates that no valid Interface Identifier is assigned to the interface. This state usually indicates that the link-local interface address failed Duplicate Address Detection. When you specify the 'Duplicate Address Detected' error flag on the interface, the new value (`noIfIdentifier(3)`) is displayed. Previously, the `snmp mib walk` command did not display the new value (`noIfIdentifier(3)`).
- **Changes in contextEngineID for SNMPv3 INFORMS (PTX Series, QFX Series, ACX Series, EX Series, MX Series, and SRX Series)**— Now the `contextEngineID` of SNMPv3 INFORMS is set to the local engine-id of Junos devices. In earlier releases, the `contextEngineID` of SNMPv3 INFORMS was set to remote engine-id.

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

Platform and Infrastructure

- **Juniper Agile Licensing (EX2300-VC, EX3400-VC, EX4300-VC, EX4400-24MP, EX4400-48MP, PTX10003, PTX10016, QFX5130-32CD, QFX5110-32Q, QFX5110-48S, QFX5120-48T, QFX5210-64C, QFX5200, and QFX5220)**—Starting from this release onwards, the Juniper Agile License Manager is deprecated. You can use the Juniper Agile Licensing Portal to activate, install, manage, and monitor licenses on Juniper Networks devices.

[See [Juniper Agile Licensing Guide](#)]

Known Limitations

IN THIS SECTION

- [Infrastructure | 25](#)
- [Platform and Infrastructure | 25](#)

Learn about known limitations in Junos OS Release 21.3R2 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

- Junos OS Release 21.1 and prior runs FreeBSD version 11 whereas from Junos OS Release 21.2 and later runs FreeBSD version 12. Software upgrade to Junos OS Release 21.1 (or later) from 21.1 (or prior) needs the `no-validate` command to be used during the software image upgrade process. (For EX4400 switches, this is applicable from Junos OS Release 21.3 and later.) [PR1586481](#)

Platform and Infrastructure

- Junos OS might become nonresponsive trying to acquire the SMP IPI lock while rebooting when it is running as a VM on Linux and QEMU hypervisor. [PR1385970](#)
- Error logs get generated when routes point to the target next hop, which in turn point to hold next hops. These error logs are present for a short time. Later, when the next hop changes from a hold next hop to valid next hop, the unilist next hops walks again, gets updated with the appropriate weight, and reroute counters. Later, no error logs get generated. [PR1387559](#)

Open Issues

IN THIS SECTION

- [Forwarding and Sampling | 26](#)
- [Interfaces and Chassis | 26](#)
- [Junos Fusion Enterprise | 26](#)
- [Platform and Infrastructure | 27](#)

Learn about open issues Junos OS Release 21.3R2 for EX Series switches.

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

Forwarding and Sampling

- The fast-lookup-filter with match that are not supported in the FLT hardware might cause the traffic to drop. [PR1573350](#)

Interfaces and Chassis

- On all Junos OS platforms with VRRP (Virtual Router Redundancy Protocol) implemented, if you configure startup-silent-period as one second and the state of any interfaces included in the VRRP-group changes, the vrrpd (VRRP daemon) to crash, impacting the related services. However, configuring startup-silent-period between two and 2000 seconds, and restarting vrrpd helps to restore the services. [PR1646480](#)

Junos Fusion Enterprise

- On a rare corner case, the Anchor IFL does not get created in time, which results in assert core during the SD provisioning state. [PR1555597](#)

Platform and Infrastructure

- When you add VLAN as an action for changing the VLAN in both the ingress and egress filters, the filter does not get installed. [PR1362609](#)
- On EX9214 switches, if the MACsec-enabled link flaps after reboot, the following error message get generated `errorlib_set_error_log(): err_id(-1718026239)`.
[PR1448368](#)
- When you run the `show pfe filter hw filter-name filter name` command, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. [PR1495712](#)
- A delay of 35 seconds gets added in the reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. [PR1514364](#)
- On all Junos OS platforms, traffic loss might be observed due to a rare timing issue when you perform frequent Interface Bridge Domain (IFBD) configuration modifications. This behavior is seen when the Packet Forwarding Engine receives out-of-order IFBD(s) from the Routing Engine and might lead to the `fxpc` process crash and drops traffic. [PR1572305](#)
- Pause frames counters do not get incremented when you send the pause frames. [PR1580560](#)
- On EX2300, EX3400, EX4300, EX4600, and EX4650 switches with the chip as the Packet Forwarding Engine, if you enable IS-IS on an IRB interface and configure the MTU size of the IRB interface with a value greater than 1496 bytes, the IS-IS hello (IIH) PDUs with jumbo frame size (that is, greater than 1496 bytes) might be dropped and not sent to the IS-IS neighbors. [PR1595823](#)
- On EX4600 switches, default configuration under `ge-0/0/*` might be missed after performing ZTP. [PR1614098](#)
- When you configure the DHCP relay mode as no-snoop on the EVPN/VXLAN environment, the offer gets dropped due to incorrect ASIC programming. [PR1530160](#)
- On EX4400-48MP switches, the virtual machine might generate core files and the Virtual Chassis might split with the multicast scale scenario. [PR1614145](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 28](#)
- [Resolved Issues: 21.3R1 | 32](#)

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.

Resolved Issues: 21.3R2

IN THIS SECTION

- [Class of Service \(CoS\) | 28](#)
- [Infrastructure | 29](#)
- [Interfaces and Chassis | 29](#)
- [Layer 2 Ethernet Services | 29](#)
- [MPLS | 29](#)
- [Platform and Infrastructure | 29](#)
- [Routing Protocols | 31](#)
- [Subscriber Access Management | 31](#)
- [Virtual Chassis | 32](#)

Class of Service (CoS)

- The dcpfe process might generate core file in the auto-channelization scenario or when you plug out SFP. [PR1616847](#)

Infrastructure

- The fxpc process might crash and generate core files. [PR1611480](#)

Interfaces and Chassis

- SNMP_TRAP_LINK_UP and SNMP_TRAP_LINK_DOWN traps might be seen while activating and deactivating firewall filters. [PR1609838](#)

Layer 2 Ethernet Services

- The jdhcpd process started spiking and DHCP becomes nonresponsive when modifying the configuration to add override always-write-giaddr and remove forward-only. [PR1618306](#)
- Option 82 might not be attached on the DHCP request packets. [PR1625604](#)

MPLS

- MPLS VPN packets drop due to missing ARP entry on the PE device. [PR1607169](#)

Platform and Infrastructure

- During flooding, MAC gets learnt only on the normal access port but not on the aggregated Ethernet interface trunk port. [PR1506403](#)
- Some transmitting packets might get dropped due to the disable-pfe action not being invoked when the fabric self-ping failure gets detected. [PR1558899](#)
- On EX2300 and EX3400 switches, the upgrade of the PoE firmware might fail. [PR1584491](#)
- During day one stage of EX4400 device management from MIST, the cloud LED remains in the Green state even if the device loses connectivity with the Cloud. [PR1598948](#)
- The l2ald process might crash due to memory leakage when all active interfaces in a VLAN becomes unstable. [PR1599094](#)
- On EX4600 switches, the SFP-T port might stop forwarding traffic. [PR1600291](#)
- NSSU performed with MACsec configuration might result in the fxpc process generating core files. [PR1603602](#)
- On EX4400 switches with POE supported device, the PoE firmware upgrade must be done with the bt-firmware command option only. [PR1606276](#)

- Change in commit might generate error message while configuring the same VLAN-ID with different VLAN name through the openconfig command. [PR1612566](#)
- FPC might crash after the device restart in the EVPN-VXLAN scenario. [PR1613702](#)
- On EX4300 switches, the OAM CFM adjacency does not get formed. [PR1619231](#)
- On EX2300, EX2300-MP, and EX3400, a slow memory leakage due to processing of the specific IPv6 packets (CVE-2022-22180) occurs. [PR1619970](#)
- EVPN Type-5 routes might not be installed. [PR1620808](#)
- Traffic might be lost after configuring VXLAN over the IRB interface. [PR1625285](#)
- Packet drop might be observed when you configure L2PT on the transit device. [PR1627857](#)
- Configuring L2PT on a transit switch in a Q-in-Q environment breaks L2PT for other S-VLANs. [PR1637249](#)
- On EX4300 switches, verification of the LOCAL-FAULT interface parameter insertion fails on the xe interface. [PR1623215](#)
- Route leakage from the primary routing-instance to the custom routing-instance failure occurs for the local interface. [PR1623429](#)
- The et-interface becomes nonresponsive and remains down between two particular ports. [PR1535078](#)
- On EX4300 devices, MAC addresses aging issue occurs. [PR1600029](#)
- Traffic loss might be observed if you configure dot1X with the supplicant multiple and authenticated user from radius in the single supplicant mode. [PR1610746](#)
- Inter-vlan connectivity might be lost in an EVPN-VXLAN with CRB topology. [PR1611488](#)
- Traffic stops when traffic switches from one LAG member to another member if you configure MACsec. [PR1611772](#)
- The EX2300, EX3400, EX4300-MP, and EX4400 devices causes MAC to move when the IGMP query packet gets received on the backup FPC port. [PR1612596](#)
- Removing the JNP-SFPP-10GE-T optical module from a port might cause certain ports to go down. [PR1614139](#)
- The Packet Forwarding Engine might crash due to deletion of storm control configuration for IFL in CLI, which might lead to traffic loss. [PR1616646](#)
- Core files might be generated on EX devices after configuration changes. [PR1618352](#)

- The dcpfe process might crash after changing and deleting the VXLAN VNI configuration on EX devices. [PR1619445](#)
- OAM CFM session does not go to the Up state if the configured ERPS and CFM control traffic uses the same VLAN as ERPS control traffic. [PR1620536](#)
- The filter required for routing the Layer 3 traffic of targeted broadcast and static ARP entry with multicast-mac address might fail to install. [PR1626620](#)
- Clients connected to the isolated VLAN through trunk port cannot communicate to the network. [PR1626710](#)
- The line card might crash and reload if the EVPN MAC entry does not get deleted correctly. [PR1627617](#)
- Unicast ARP packets with the first four bytes of its destination MAC matching to system MACs of a transit system gets trapped by the system. [PR1632643](#)
- On EX3400 Virtual Chassis, traffic loss for 20 seconds occur when you reboot the backup FPC with the static link-protection. [PR1633115](#)
- The VCPs connected with the AOC cable might not come up after upgrading to Junos OS Release 17.3 or later. [PR1633998](#)
- MAC address might not be learned on the new interface after moving the MAC. [PR1637784](#)
- MAC-move might be observed when you configure dhcp-security. [PR1639926](#)
- On EX4600 switches, the interface on SFP-T or SFP-SX might stop forwarding traffic. [PR1598805](#)
- The Packet Forwarding Engine might get crash when the Virtual Chassis member flaps. [PR1634781](#)
- Delay might be observed for the interfaces to come up after reboot or transceiver replacement. [PR1638045](#)

Routing Protocols

- The rpd process might generate core file due to memory corruption. [PR1599751](#)
- The rpd process might crash and restart when you enable NSR. [PR1620463](#)

Subscriber Access Management

- Adding the new radius access configuration might fail. [PR1629395](#)

Virtual Chassis

- During NSSU, errors related to link might be observed while you attach or detach IFDs. [PR1622283](#)
- Delay might be observed while establishing the virtual-chassis post upgrading or rebooting device. [PR1624850](#)

Resolved Issues: 21.3R1

IN THIS SECTION

- General Routing | [32](#)
- Class of Service (CoS) | [35](#)
- EVPN | [35](#)
- Infrastructure | [36](#)
- Interfaces and Chassis | [36](#)
- Junos Fusion Enterprise | [36](#)
- Layer 2 Features | [36](#)
- Layer 2 Ethernet Services | [36](#)
- Platform and Infrastructure | [36](#)
- Routing Protocols | [37](#)
- Virtual Chassis | [37](#)

General Routing

- In EX2300 and EX3400 platforms, RTC ERROR and SETTIME failed messages are noted. [PR1535106](#)
- The Power over Ethernet (POE) might fail on EX platforms due to a rare timing issue in the Virtual Chassis scenario. [PR1539933](#)
- **Cattle-Prod Daemon received unknown trigger (type Semaphore, id 1)** error messages seen on the vty when the CLI commands to fetch host route scale are issued. [PR1554140](#)
- The Virtual Chassis Port (VCP) might not come up EX4600 platform. [PR1555741](#)
- FPC with power related faults might come online again after Fabric Healing sets the FPC offline. [PR1556558](#)

- The MAC addresses learned in a Virtual Chassis might fail, aging out in MAC scaling environment. [PR1558128](#)
- Some transmitting packets might get dropped due to the **disable-pfe** action is not invoked when the fabric self-ping failure is detected. [PR1558899](#)
- The DHCP client might not obtain IP address when dhcp-security is configured. [PR1564941](#)
- On EX platforms, the new primary Routing Engine post switchover might go into DB mode (or crash). [PR1565213](#)
- The rpd crash might be seen at boot time. [PR1567043](#)
- The 40G DAC connection between EX9253 and the peers might not come up. [PR1569230](#)
- On a EX4400 Virtual Chassis, the SNMP MIB object jnRedundencySwitchOverCount will not be reset to 0 when the entire Virtual Chassis is rebooted. [PR1570359](#)
- Packet loss might be observed when sample based action is used in firewall filter. [PR1571399](#)
- Private VLAN configuration might fail in certain scenario. [PR1574480](#)
- Protocol convergence between end nodes might fail when L2PT is enabled on transit switch. [PR1576715](#)
- The device implemented with different service image version might become VC member as unexpected. [PR1576774](#)
- The fxpc process might crash on EX Series platforms. [PR1578421](#)
- The dcpfe crash is observed on Junos EX platforms. [PR1578859](#)
- Random/silent reboot might be seen on EX2300-24MP and EX2300-48MP platforms. [PR1579576](#)
- On the EX Series platforms, a few 40G ports might not be channelized successfully. [PR1582105](#)
- The voice VLAN might not get assigned to the access interface. [PR1582115](#)
- The l2ald crash if a specific naming format is applied between a vlan-range and a single vlan. [PR1583092](#)
- When EX2300-MP in standalone mode is used as a DHCP server, initial set of packets received in the server might get dropped. [PR1583983](#)
- DSCP rewriting might fail to work on EX2300 switches. [PR1586341](#)
- Packet drops during VRRP primary reboot when 40XS linecard is present on some EX9204 platforms. [PR1586740](#)

- The SNMP trap for MAC notifications might not be generated when an interface is added explicitly under switch-options. [PR1587610](#)
- Process dot1xd crash might be seen and re-authentication might be needed on EX9208 platform. [PR1587837](#)
- The rpd crash might be observed on the router running a scaled setup. [PR1588439](#)
- Packet loss could be observed on dynamically assigning VoIP VLAN. [PR1589678](#)
- Traffic loss might be observed for interface configured in subnet 137.63.0.0/16. [PR1590040](#)
- Inconsistent statistics value seen on performing **slaac-snooping**. [PR1590926](#)
- The LLDP packet might lose on the EX-4300MP platform if LLDP is configured on the management interface. [PR1591387](#)
- The show pfe filter hw might generate **ERROR (dfw): Unknown group id: 21** message. [PR1592096](#)
- The DHCP relay might not work if it connects with the server via type 5 route which with aggregated Ethernet interface as the underlay interface. [PR1592133](#)
- On all Junos platforms, xSTP might not get configured when enabled on an interface with SP style configuration. [PR1592264](#)
- On the EX4300-48MP Virtual Chassis, the backup Routing Engines clear the reporting alarm for a PEM failure intermittently for a missing power source. [PR1593795](#)
- Clients authentication failure might occur due to dot1x daemon memory leak. [PR1594224](#)
- Storm control profile might not be applied on EX2300 platforms. [PR1594353](#)
- On a EX4400 VC, log messages related to fan settings will be observed in chassis traceoptions file. [PR1594446](#)
- The MAC/IP withdraw route might be suppressed by rpd in the EVPN-VxLAN scenario. [PR1597391](#)
- The backup Virtual Chassis member might not learn MAC address on a primary after removing a VLAN unit from the SP style aggregated Ethernet interface which is part of multiple VLAN units. [PR1598346](#)
- On EX4400 Virtual Chassis, linecard member console might fail to redirect to Virtual Chassis primary. [PR1599625](#)
- Unable to disable the management port em1. [PR1600905](#)
- EX4400 PVIDB schema files not updated for the correct count of (lic_ft_cnt) Licensing feature. [PR1601449](#)

- On EX2300 and EX4650, if the system is upgraded from 20.2 or earlier release to 20.3 or later release, either using phone-home feature or when the system is in factory default state, the upgrade will fail with phone-home crash. [PR1601722](#)
- On EX2300 Virtual Chassis platforms ARP might not get resolved. [PR1602003](#)
- On a EX4400 Virtual Chassis, the Cloud LED will display pattern for **NO_CLOUD_RESPONSE** when there is no IP address present on IRB interface or no DNS is configured on the device. [PR1602664](#)
- On EX4400 dot1x authentication might not work on EVPN/xlan enabled endpoints. [PR1603015](#)
- The NSSU performed with MACsec configuration might result in fxpc core. [PR1603602](#)
- MAC move might be seen between the ICL and MC-LAG interface if adding or removing VLANs on the ICL interface. [PR1605234](#)
- On EX and QFX Series switches, the fxpc process might crash and generate a core dump. [PR1607372](#)
- On EX4300 platform, the dcpfe process might crash and generate core. [PR1608306](#)
- DHCP packets might be received and then returned back to DHCP relay through the same interface on EX2300/EX3400/EX4300 platforms. [PR1610253](#)
- After performing NSSU, **timeout waiting for response from fpc0** error message is seen while checking version detail. [PR1584457](#)
- There is a steady increase in storage usage in the backup chassis when the subscriber service is enabled. [PR1595238](#)

Class of Service (CoS)

- The buffer allocation for VCP ports might not get released in Packet Forwarding Engine after physically moving the port location. [PR1581187](#)

EVPN

- Traffic loss might be seen under EVPN-VxLAN scenario when MAC-IP moves from one CE interface to another. [PR1591264](#)
- The label field for the EVPN Type 1 route is set to 1. [PR1594981](#)
- Traffic loss might be seen if aggregated Ethernet bundle interface with ESI is disabled on primary Routing Engine followed by a Routing Engine switchover. [PR1597300](#)

Infrastructure

- While loading the kernel displays the following error message: **GEOM: mmcsd0s.enh: corrupt or invalid GPT detected.** [PR1549754](#)
- The vme/me0 management interface cannot process any incoming packets. [PR1552952](#)
- Some MAC addresses might not be aged out on EX4300 platforms. [PR1579293](#)
- In EX4400 platforms, under some conditions, the FPGA reset reason might be incorrectly shown in console logs as 0. [PR1579331](#)
- The fxpc process might crash and generate core. [PR1611480](#)

Interfaces and Chassis

- The aggregated Ethernet interface might flap. [PR1576533](#)
- ARP resolution failure might occur during VRRP failover. [PR1578126](#)
- VRRP incorrect advertisement threshold values are seen on vrrp groups when VRRP is configured on EX2300 boxes. [PR1584499](#)

Junos Fusion Enterprise

- Reverting mastership from RE1 to RE0 might lead to l2ald daemon crash and cause an outage. [PR1601817](#)

Layer 2 Features

- MAC addresses learnt from the MC-LAG client device might keep flapping between the ICL interface and MC-AE interface after one child link in the MC-AE interface is disabled. [PR1582473](#)

Layer 2 Ethernet Services

- The DHCP client will be offline for 120 seconds after sending the DHCPINFORM message in the DHCP relay scenario. [PR1575740](#)
- The DHCP client might be offline for about 120 seconds after sending the DHCPINFORM message. [PR1587982](#)

Platform and Infrastructure

- On Ex3400 VC, console access on backup VC member is not allowed. [PR1530106](#)

- Junos OS: Upon receipt of specific sequences of genuine packets destined to the device the kernel will crash and restart (vmcore) (CVE-2021-0283, CVE-2021-0284). [PR1557881](#)
- On all EX9200 platforms with EVPN-VXLAN configured, the next hop memory leak in MX Series ASIC happens whenever there is a route churn for remote MAC-IP entries learned bound to the IRB interface in EVPN-VXLAN routing instance. When the ASIC's next hop memory partition is exhausted, the FPC might reboot. [PR1571439](#)
- FPC crashes might be seen on EX92 platforms. [PR1579182](#)
- The pfex might crash during PIC 4x 1G/10G SFP/SFP+ offline/online. [PR1582457](#)
- Firewall filter is not programmed correctly and traffic would be dropped unexpectedly. [PR1586433](#)
- The Egress RACL Firewall filter might not get programmed correctly on EX4300 platforms. [PR1595797](#)
- Broadcast traffic might be discarded when a firewall filter is applied to the loopback interface. [PR1597548](#)
- VLAN tagged traffic might be dropped with service provider style configuration. [PR1598251](#)
- The VRRP packets might not be forwarded when **mac-move-limit** configuration statement is configured. [PR1601005](#)
- Adding aggregated Ethernet configuration without child member might cause MAC or ARP learning issues. [PR1602399](#)
- ZTP does not work when downgrade from 21.1R2.2 image to 21.1R2.1 image. [PR1603227](#)
- Slaac-Snooping global address entry learnt over vtep interface does not RENEW sometimes after lease timer expiry. [PR1603269](#)

Routing Protocols

- BGP session carrying VPNv4 prefix with IPv6 next-hop might be dropped. [PR1580578](#)
- The rpd might crash in scaled routing instances scenario. [PR1590638](#)

Virtual Chassis

- EX4300 VCP might not come up after upgrade when QSFP+-40G-SR4/QSFP+-40G-LR4/QSFP+40GE-LX4 is used. [PR1579430](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R2 documentation for EX Series switches.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 38

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 2: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the [Installation and Upgrade Guide](#).

Junos OS Release Notes for JRR Series

IN THIS SECTION

- [What's New | 40](#)
- [What's Changed | 41](#)
- [Known Limitations | 41](#)
- [Open Issues | 41](#)
- [Resolved Issues | 42](#)
- [Documentation Updates | 43](#)
- [Migration, Upgrade, and Downgrade Instructions | 43](#)

These release notes accompany Junos OS Release 21.3R2 for the JRR Series Route Reflectors. 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

- [What's New in 21.3R2](#) | 40
- [What's New in 21.3R1](#) | 40

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

What's New in 21.3R2

There are no new features or enhancements to existing features in Junos OS Release 21.3R2 for JRR.

What's New in 21.3R1

IN THIS SECTION

- [Routing Protocols](#) | 40

Routing Protocols

- **BMP with BGP Sharding and Update IO (JRR Series, MX Series, PTX Series, and vMX)**— Starting in Junos OS Release 21.3R1, we support AdjOutRIBs (pre and post policy tables) through BGP Monitoring Protocol (BMP).

[See [BGP Monitoring Protocol](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.3R2 | 41](#)

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

What's Changed in Release 21.3R2

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 and 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 Junos OS Release 21.3R2 for JRR Series Route Reflectors.

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

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 42](#)
- [Resolved Issues: 21.3R1 | 42](#)

Learn about the issues fixed in this release for JRR Series Route Reflectors.

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

Resolved Issues: 21.3R2

IN THIS SECTION

- [General Routing | 42](#)

General Routing

- On JRR200, monitor traffic interface doesn't work on em2. [PR1629242](#)

Resolved Issues: 21.3R1

IN THIS SECTION

- [General Routing | 42](#)

General Routing

- On JRR200, incorrect Power Entry Module (PEM) load percentage is observed when you execute show chassis power CLI command. [PR1598728](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R2 documentation for JRR Series Route Reflectors.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 43

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

For information about software installation and upgrade, see the [JRR200 Route Reflector Quick Start](#) and [Installation and Upgrade Guide](#).

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

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

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

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

IN THIS SECTION

- [What's New | 45](#)
- [What's Changed | 46](#)
- [Known Limitations | 46](#)
- [Open Issues | 46](#)
- [Resolved Issues | 46](#)
- [Documentation Updates | 46](#)

These release notes accompany Junos OS Release 21.3R2 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

- [What's New in 21.3R2](#) | 45
- [What's New in 21.3R1](#) | 45

Learn about new features introduced in this release for Juniper Secure Connect.

What's New in 21.3R2

There are no new features or enhancements to existing features in Junos OS Release 21.3R2 for Juniper Secure Connect.

What's New in 21.3R1

IN THIS SECTION

- [Additional Features](#) | 45

Additional Features

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

- **Juniper Secure Connect and NCP Exclusive Remote Access Client with ikev2 process** (SRX5000 line of devices with SPC3 and vSRX 3.0 running ikev2)

[See [Juniper Secure Connect](#) and [Remote Access VPNs with NCP Exclusive Remote Access Client](#).]

What's Changed

Learn about what changed in this release for Juniper Secure Connect.

Known Limitations

There are no known limitations in hardware and software in Junos OS 21.3R2 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 and software in Junos OS Release 21.3R2 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

Learn about the issues fixed 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.

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R2 documentation for Juniper Secure Connect.

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

- [What's New | 47](#)
- [What's Changed | 47](#)
- [Known Limitations | 48](#)
- [Open Issues | 48](#)
- [Resolved Issues | 48](#)
- [Documentation Updates | 49](#)
- [Migration, Upgrade, and Downgrade Instructions | 49](#)

These release notes accompany Junos OS Release 21.3R2 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 Releases 21.3R1 or 21.3R2 for Junos fusion for enterprise.

What's Changed

There are no changes in behavior and syntax in Junos OS Releases 21.3R1 or 21.3R2 for Junos fusion for enterprise.

Known Limitations

There are no known limitations in hardware or software in Junos OS Release 21.3 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 Junos OS Release 21.3 for Junos fusion for enterprise.

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

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 48](#)
- [Resolved Issues: 21.3R1 | 49](#)

Learn about the issues fixed in these releases 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: 21.3R2

There are no fixed issues in the Junos OS Release 21.3R2 for Junos fusion for enterprise.

Resolved Issues: 21.3R1

IN THIS SECTION

- [Junos fusion for enterprise | 49](#)

Junos fusion for enterprise

- Reverting mastership from RE1 to RE0 might cause the l2ald daemon to generate a core file.
[PR1601817](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R2 documentation for Junos fusion for enterprise documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading Junos OS on an Aggregation Device | 50](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 51](#)
- [Preparing the Switch for Satellite Device Conversion | 52](#)
- [Converting a Satellite Device to a Standalone Switch | 54](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 54](#)
- [Downgrading Junos OS | 55](#)

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 4: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the [Installation and Upgrade Guide](#).

Downgrading Junos OS

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

NOTE: You cannot downgrade more than three releases.

For more information, see the [Installation and Upgrade Guide](#).

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

Junos OS Release Notes for Junos Fusion for Provider Edge

IN THIS SECTION

- [What's New | 56](#)
- [What's Changed | 56](#)
- [Known Limitations | 56](#)
- [Open Issues | 56](#)
- [Resolved Issues | 57](#)
- [Documentation Updates | 57](#)
- [Migration, Upgrade, and Downgrade Instructions | 58](#)

These release notes accompany Junos OS Release 21.3R2 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 this release for Junos Fusion for provider edge.

What's Changed

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

Known Limitations

There are no known limitations in hardware and 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 open issues in hardware and 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

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 57](#)

There are no resolved issues in this release for Junos Fusion for provider edge.

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

Resolved Issues: 21.3R2

IN THIS SECTION

- [Junos Fusion Provider Edge | 57](#)

Junos Fusion Provider Edge

- Configuring port mirroring firewall filter in a bridge domain with IRB might cause traffic loss over IRB. [PR1607750](#)

Documentation Updates

There are no errata or changes in Junos OS Release 21.3R2 documentation for Junos Fusion for provider edge documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading an Aggregation Device | 58](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 61](#)
- [Preparing the Switch for Satellite Device Conversion | 61](#)
- [Converting a Satellite Device to a Standalone Device | 63](#)
- [Upgrading an Aggregation Device | 66](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 66](#)
- [Downgrading from Junos OS Release 21.3 | 67](#)

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 21.3R2 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/jinstall64-21.3R2.SPIN-
domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.3R2.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/jinstall64-21.3R2.SPIN-
export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.3R2.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 21.3R2 `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, unbundle 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 21.3R1, 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 5: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the [Installation and Upgrade Guide](#).

Downgrading from Junos OS Release 21.3

To downgrade from Release 21.3 to another supported release, follow the procedure for upgrading, but replace the 21.3 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the [Installation and Upgrade Guide](#).

Junos OS Release Notes for MX Series

IN THIS SECTION

- [What's New | 68](#)
- [What's Changed | 78](#)
- [Known Limitations | 83](#)
- [Open Issues | 85](#)
- [Resolved Issues | 96](#)
- [Documentation Updates | 136](#)
- [Migration, Upgrade, and Downgrade Instructions | 136](#)

These release notes accompany Junos OS Release 21.3R2 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

- [What's New in 21.3R2 | 68](#)
- [What's New in 21.3R1 | 68](#)

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

What's New in 21.3R2

There are no new features or enhancements to existing features in Junos OS Release 21.3R2 for MX Series routers.

What's New in 21.3R1

IN THIS SECTION

- [Hardware | 69](#)
- [Chassis | 69](#)
- [IP Tunneling | 69](#)
- [IPv6 | 70](#)
- [Junos Telemetry Interface | 70](#)
- [Layer 2 VPN | 71](#)
- [MPLS | 71](#)
- [Network Address Translation \(NAT\) | 72](#)
- [Platform and Infrastructure | 72](#)
- [Routing Options | 72](#)
- [Routing Protocols | 73](#)
- [Source Packet Routing in Networking \(SPRING\) or Segment Routing | 74](#)
- [Subscriber Management and Services | 75](#)
- [System Management | 76](#)
- [VPNs | 76](#)

Hardware

- **Support for new line card, LC2103-V2 in MX10003 routers** —In Junos OS Release 21.3R1, we've introduced a new line card, LC2103-V2 (model number MX10K3-L2103B-BASE) for our MX10003 routers. Equipped with a new four-core CPU, the line card ensures better broadband gateway performance with increased cps values. [See [Hardware Compatibility Tool](#).]
- **Support for QSFP-100G-LR and QSFP-100G-FR transceivers (MX10008 with the MX10K-LC2101 line card)**—Starting in Junos OS Release 21.3R1, the MX10008 routers with the MX10K-LC2101 line card support the QSFP-100G-LR and QSFP-100G-FR transceivers.

[See [Hardware Compatibility Tool](#).]

Chassis

- **Support for MX-SPC3 in MX Series Virtual Chassis (MX240, MX480, and MX960 with MX-SPC3)**—Starting in Junos OS Release 21.3R1, we support the MX-SPC3 service card in an MX Series Virtual Chassis setup for NAT, stateful firewall, and IDS features. However, you cannot configure aggregated multiservices (AMS) bundles with MX-SPC3 service cards on both the chassis.

The maximum number of MX-SPC3 service cards that each chassis (in the Virtual Chassis setup) supports for different devices is as follow:

- MX240: 2
- MX480: 5
- MX960: 7

[See [Virtual Chassis Components Overview](#) .]

IP Tunneling

- **Support for IP-over-IP tunnel stitching (MX Series, MX240, MX480, MX960, PTX1000, PTX10008, PTX10016, and QFX10002)**—In Junos OS Release 21.3R1, we introduce IP-over-IP tunnel stitching. You can use this feature to terminate an IP-over-IP tunnel on a device and initiate another tunnel on the same device. When a device receives the IP-over-IP packet, it de-encapsulates the outer packet header and inner packet lookup occurs. The inner IP packet header then points to another tunnel on

the same device, where the same device encapsulates the packet again with another IP-over-IP header.

[See [Overview of Next-Hop-Based Dynamic Tunneling Using IP-Over-IP Encapsulation.](#)]

IPv6

- **PCEP session over IPv6 (MX480, MX960, and MX10003)**—Starting in Junos OS Release 21.3R1, we've extended the Path Computation Element Protocol (PCEP) session management over IPv6. With this support, Path Computation Client (PCC) and Path Computation Element (PCE) can establish an IPv6 session with or without TCP MD5 hash.

Junos OS can set up an IPv6 PCEP session with NorthStar, Paragon Pathfinder, or a third-party controller if it is capable of establishing an IPv6 session. The IPv6 session supports functionalities such as PCE-provisioned LSPs, PCE-delegated LSPs, router-controlled LSPs, and LSP synchronization over an IPv6 PCEP session with or without MD5 security.

You cannot configure PCE with both IPv4 address and IPv6 address; only one address format is supported at a time.

[See [destination-ipv6-address](#) and [local-ipv6-address](#).]

Junos Telemetry Interface

- **Telemetry stream path resolution by MPLS and RSVP interfaces (ACX710, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5448, ACX4558-D, ACX5448-M, MX150, MX204, MX340, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, vMX, PTX1000, PTX3000, PTX5000, PTX10002-60C, and PTX10008)**—Starting in Junos OS Release 21.3R1, you can choose to stream telemetry statistics only for MPLS and RSVP-enabled interfaces. Use the resource path `/network-instances/network-instance/mpls/signaling-protocols/rsvp-te/interface-attributes/interface/admin-status`.

[See [Configuring a Junos Telemetry Interface Sensor \(CLI Procedure\)](#) and [Telemetry Sensor Explorer](#).]

- **Inline video monitoring statistics (MX240, MX480, MX960, MX2010, and MX2020 routers with MPC10 or MPC11 line cards)**—Starting in Junos OS Release 21.3R1, you can use new sensors to stream video monitoring related statistics and MDI flow alarms generated to an outside collector by means of remote procedure call (gRPC) or gRPC Network Management Interface (gNMI). Statistics and alarms are provided for each configured line card. Use the resource paths `/junos/system/linecard/services/vmon-mdi/` and `/junos/system/linecard/services/vmon-mdi-alarm/`.

[See [Telemetry Sensor Explorer](#).]

- **Abstracted fabric interface support (MX2010 and MX2020 with MPC11 line cards)**—Starting in Junos OS Release 21.3R1, JTI sensor support is extended to MPC11 line cards for abstracted fabric interfaces. The routers support this sensor only for node virtualization configurations where an

abstract fabric Interface is the connecting link between guest network functions (GNFs). The JTI sensor reports:

- Interface-specific load-balancing and fabric queue statistics.
- Aggregated statistics across all abstracted fabric interfaces hosted on a source Packet Forwarding Engine of local GNFs.
- Fabric statistics for all traffic arriving from the fabric interfaces on the local GNF Packet Forwarding Engine and exiting to the fabric on that Packet Forwarding Engine.

The MX2010 and MX2020 support the sensor through gRPC and UDP (native). Use the resource path `/junos/system/linecard/node-slicing/af-fab-stats/` to configure the JTI sensor.

To provision the sensor to export data through gRPC, use the `telemetrySubscribe` RPC to specify telemetry parameters.

For UDP native export of statistics, configure parameters at the `[edit services analytics]` hierarchy level.

[See [sensor \(Junos Telemetry Interface\)](#), [Configuring a Junos Telemetry Interface Sensor \(CLI Procedure\)](#), and [Telemetry Sensor Explorer](#).]

Layer 2 VPN

- **Control word on the MPC-10E line card (MX Series)**—Starting in Junos OS Release 21.3R1, MPC-10E line cards support the insertion of a control word between the label stack and the Layer 2 payload for VPLS services. You can use the control word to prevent provider edge routers from incorrectly identifying a VPLS payload as an IPv4 or IPv6 payload. You also prevent out-of-order packet delivery in a VPLS network that is configured to load-balance VPLS traffic across multiple paths. To enable the control word, include the `control-word` statement at the `[edit routing-instances routing-instance-name protocols vpls]` hierarchy level.

[See [Control Word for BGP VPLS Overview](#).]

MPLS

- **RSVP updates available bandwidth values without notifying IS-IS (MX960, MX2010, MX2020, PTX1000, PTX10001, PTX10008, and PTX10016)**—When RSVP label-switched paths (LSPs) and segment routing LSPs coexist on a link, RSVP takes into account how much bandwidth the segment routing LSPs use. By default, RSVP updates the values for the local unreserved bandwidth and the maximum available bandwidth and passes the values on to IS-IS. Starting in Junos OS Release 21.3R1, you can configure RSVP to update available bandwidth values without notifying IS-IS if the bandwidth change is within a certain threshold configured at the `[edit protocols rsvp interface interface-name update-threshold-max-reservable]`.

If you configure the `local-bw-override-threshold` statement at the `[edit protocols rsvp interface interface-name non-rsvp-bandwidth]` hierarchy level, RSVP always updates the available bandwidth values. However, it reports only the new values to IS-IS if the bandwidth change passes the threshold.

[See [update-threshold-max-reservable](#) and [local-bw-override-threshold](#).]

- **Maximum ECMP paths using MPLS-over-UDP encapsulation (MX Series)**—Starting in Junos OS Release 21.3R1, you can set the maximum number of ECMP paths supported using MPLS-over-UDP tunnels 128. Every time a UDP tunnel is configured a tunnel composite next hop is created.

[See [Understanding BGP Multipath](#).]

Network Address Translation (NAT)

- **Support for NAT-T on MX-SPC3 (MX240, MX480, and MX960 with MX-SPC3)**— Starting in Junos OS Release 21.3R1, the MPC10E (MPC10E-15C-MRATE and MPC10E-10C-MRATE) line card interoperates with the MX-SPC3 service card to support NAT-T.

[See [Route-Based and Policy-Based VPNs with NAT-T](#).]

Platform and Infrastructure

- **Support for MACsec and timing on MX10K-LC480 (MX10008 and MX10016)**— Starting in Junos OS Release 21.3R1, we support MACsec and timing feature with precision time protocol (PTP) g8275.1 profile on MX10K-LC480 line card.

[See [Protocols and Applications Supported by MX10K-LC480 for MX Series Routers](#).]

Routing Options

- **Enhanced PPPoE session creation on backup router (MX Series devices and vMX)**—In Junos OS releases before Release 21.3R1, the PPPoE session switch over from a primary router to a backup router happens after the Point-to-Point Protocol (PPP) keepalive time expires. Starting in Junos OS Release 21.3R1, the PPPoE session can switch over without waiting for the keepalive time to expire. When the backup router receives an unrecognized packet from a PPP session, it responds with PPPoE Active Discovery Termination (PADT) message. This PADT response causes the PPP client to restart immediately, which reduces the time to restart PPP sessions.

This enhancement allows the subscribers to quickly reestablish the session on the standby router.

[See [Understanding Point-to-Point Protocol over Ethernet](#).]

Routing Protocols

- **Check for AS match in BGP policy AS paths without using regular expressions (ACX5048, ACX5096, ACX5448, MX240, MX480, MX960, MX2008, MX10016, vMX, PTX1000, PTX5000, PTX10001, PTX10002, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, and QFX10016)**—Starting in Junos OS Release 21.3R1, you can configure BGP policies to check for an autonomous system (AS) match in an AS path without using regular expressions. The BGP policy compares the AS to an AS-list or AS-list-group and returns true if it finds a match. You can configure the BGP policy to check for a matching origin, neighbor, or transit AS. This feature provides a faster alternative to match origin, transit, and peer AS numbers than using a regular expression.

Configure this feature using the `as-path-neighbors`, `as-path-origins`, or `as-path-transits` option at the [edit policy-options policy-statement *policy-name* from] hierarchy level. For each type of match, use (as-list | as-list-group) *as-list-name/as-list-group-name* to specify the list or group of AS paths to compare the match to. Configure the AS list or AS group at the [edit policy-options] hierarchy level.

[See [policy-options](#) and [policy-statement](#).]

- **Maximum reference bandwidth increased to 4 TB for IGP protocols (ACX710, ACX5448, MX960, MX2020, MX10003, PTX5000, and PTX1000)**—Starting in Junos OS Release 21.3R1, we've increased the maximum reference bandwidth for IS-IS and OSPF IGP protocols from 1 Tbps to 4 Tbps. The default bandwidth is 100 Mbps. You can increase the reference bandwidth to adjust the path metrics, which you use to determine the preferred path in case of multiple equal-cost routes to a destination.

To configure the reference bandwidth, use the `reference-bandwidth` *reference-bandwidth* statement at the [edit protocols isis] hierarchy level or the [edit protocols (ospf | ospf3)] hierarchy level.

[See [reference-bandwidth \(Protocols IS-IS\)](#) and [reference-bandwidth \(Protocols OSPF\)](#).]

- **Support for route target (RT) multipath (MX Series and PTX Series)**—Starting in Junos OS Release 21.3R1, the BGP RIB sharding supports route target (RT) multipath and dependent features such as protect-core and policy-based multipath. RT multipath does load balancing by combining next hops from multiple component routes to form a forwarding-only route. When you enable sharding, both the shard and the main threads participates in this process of creating the forwarding-only route.
- **Support for SRv6 in BGP-LS and Traffic Engineering Database (MX204, MX960, MX10003 and MX10008)** —Starting in Junos OS Release 21.3R1, we support SRv6 in BGP-LS and Traffic Engineering Database (TED). BGP-LS extensions export the SRv6 topology information to the SDN controllers. Controllers receive the topology information by being part of an IGP domain or through BGP-LS.

You can filter NLRIs based on IPv6 prefix (SRv6 Locator) and SRv6 SID NLRIs.

To filter NLRIs based on IPv6 prefix, use `ipv6-prefix` at the [edit policy-options policy-statement name from traffic-engineering] hierarchy level.

To filter NLRIs based on SRv6 SID, use `srv6-sid` at the `[edit policy-options policy-statement name from traffic-engineering]` hierarchy level.

[See [Link-State Distribution using SRv6](#), [ipv6-prefix](#) and [srv6-sid](#).]

- **BMP with BGP Sharding and Update IO (JRR Series, MX Series, PTX Series, and vMX)**— Starting in Junos OS Release 21.3R1, we support AdjOutRIBs (pre and post policy tables) through BGP Monitoring Protocol (BMP).

[See [BGP Monitoring Protocol](#).]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **SRv6 support for static SR-TE policy (MX204, MX960, MX10003, and MX10008)**—Starting in Junos OS Release 21.3R1, you can configure static segment routing-traffic engineering (SR-TE) tunnels over an SRv6 data plane.

Use the following configuration commands to enable SRv6 support:

- For an SR-TE policy: `set protocols source-packet-routing srv6`
- For an SR-TE tunnel: `set protocols source-packet-routing source-routing-path lsp name srv6`
- For an SR-TE segment list: `set protocols source-packet-routing source-routing-path segment-list srv6`

[See [Understanding SR-TE Policy for SRv6 Tunnel](#).]

- **Avoid microloops in IS-IS segment routing MPLS networks (MX Series routers with MPC7E, MPC8E and MPC9E line cards)** —Starting in Junos OS Release 21.3R1, you can enable post-convergence path calculation on a device to avoid microloops between network devices. Microloops form when a network change such as a link or metric change occurs in a segment routing MPLS network. A network change might trigger a loop between upstream and downstream routers for a brief time period because the routers do not update their forwarding state simultaneously.

To configure microloop avoidance in a segment routing MPLS network, include the `maximum-labels` and the `maximum-srv6-sids` statements at the `[edit protocols isis spf-options microloop-avoidance post-convergence-path]` hierarchy level.

[See [Understanding Microloop Avoidance](#).]

- **Support for Application Specific Link Attributes (ASLA) for flexible algorithms (ACX710, MX204, MX240, MX480, MX960, MX10003, MX 10008, MX10016, MX2008, MX2010, MX2020, PTX1000, PTX5000, PTX10002, PTX10008, PTX10016, VMX)**: IS-IS supports advertising different te-metric and admin-groups for RSVP and flexible algorithm on the same link using flexible-algorithm specific ASLA as defined in RFC 8919.

[See **strict-asla-based-flex-algorithm**<https://www.juniper.net/documentation/us/en/software/junos/is-is/topics/ref/statement/protocols-isis-source-packet-routing-strict-asla-based-flex-algorithm.html>.]

Subscriber Management and Services

- **Access profile support per VLAN in a domain (MX Series devices and vMX)**—Starting in Junos OS Release 21.3R1, you can configure subdomains under a domain map. In a subdomain, you can configure access profiles per VLAN or for a VLAN range. This enhancement gives you the flexibility to differentiate the users in a domain and to provide different services based on the users' profiles.

[See [map \(Domain Map\)](#) and [sub-domain](#).]

- **Enhancement to line cards for broadband edge (MX10003)**—Starting in Junos OS Release 21.3R1, we've enhanced the line cards on the MX10003 to significantly improve the calls per second (CPS) for subscriber services.

These are the enhancements to the line cards:

- Four 2.4-GHz Ranglely CPUs
- Improved clock rate for the external DRAM

[See [MX10003 Routing and Control Board](#).]

- **Junos Multi-Access User Plane support for SGW-U and PGW-U co-location (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 21.3R1, Junos Multi-Access User Plane provides a long-route implementation as a replacement for a filter-based implementation to steer traffic to the anchor Packet Forwarding Engine. The benefits are:
 - An external loopback connection to forward data when both the SGW-U and PGW-U are co-located in the same MX Series router is no longer necessary.
 - The firewall configuration to filter and route GTP packets to the anchor PFE is no longer necessary.

You do not need to make any CLI configuration changes to take advantage of this enhancement. However:

- You can remove the firewall filter for GTP packets.
- To optimize throughput of 4G traffic, you can attach a specific 4G gateway type (PGW-U or SGW-U) to a specific anchor PFE by adding the new `colocated-4g-pgw` or `colocated-4g-sgw` option at the [edit services mobile-edge gateways saegw system anchor-pfes interface interface-name] hierarchy level.

[See [Junos Multi-Access User Plane Overview](#).]

- **CHAP password override in RADIUS Access-Request message (MX Series, vMX Series)**—Starting in Junos OS Release 21.3R1, you can configure a CHAP password to override the existing password for authenticating any subscriber associated with the domain map. The override CHAP password replaces the CHAP challenge response from the PPPoE client when it attempts authentication.

[See [Changing the User Name and Password to Simplify Off-Chassis Provisioning.](#)]

- **Support for RPF counters at Ethernet interface level (MX Series)**—Starting in Junos OS Release 21.3R1, you can view RPF counters at the Ethernet interface level. To enable RPF counters at the Ethernet interface level, configure the `rpf-stats` statement at the `[edit interfaces interface-name]` hierarchy level. You can view and clear the RPF counters using the following commands, respectively:

- `show interfaces if-name extensive/detail`
- `clear interfaces statistics if-name`

[See [fields \(for Interface Profiles\)](#), [show interfaces statistics](#), and [clear interfaces statistics](#).]

- **NAS-Port-ID format enhancement (MX Series devices and vMX)**—In Junos OS Release 21.3R1, we've introduced a new NAS-Port-ID format for RADIUS server access request. The new NAS-Port-ID format is **S-VLAN<concatenated 0's>C-VLAN:S-VLAN-C-VLAN**. For a C-VLAN, if the number of digits is less than four, precede it with zeros. For example, NAS-Port-ID for S-VLAN 72 and C-VLAN 82 is 720082:72-82.

You can configure the `fixed-size-inner-tag` and `fixed-size-outer-tag` statements at the `[edit access profile profile-name radius options nas-port-id-format concatenated-vlan-tags]` hierarchy level.

[See [nas-port-id-format](#).]

System Management

- **Network Time Security (NTS) support for Network Time Protocol (NTP) (EX Series, MX Series, NFX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 21.3R1, NTS provides cryptographic security for network time synchronization and supports the client/server mode of NTP. NTS uses the Transport Layer Security (TLS) protocol and Authenticated Encryption with Associated Data (AEAD) to obtain network time in an authenticated manner.

NTS provides strong cryptographic protection against wide range of security attacks such as packet manipulation, spoofing, DDOS amplification attacks, and replay attacks. NTS also provides scalability as servers can serve several clients without the need for any manual client-specific preconfiguration.

[See [Network Time Security \(NTS\) Support for NTP](#).]

VPNs

- **Support for IPsec tunnel MTU (MX240, MX480, and MX960 with MX-SPC3, SRX5400, SRX5600, and SRX5800 with SPC3, and and vSRX devices)**— Starting in Junos OS Release 21.3R1, you can

configure the MTU size for IPsec tunnels. This configuration defines the maximum size of an IP packet, including the IPsec overhead.

On IPv6, we provide support to disable the ICMPv6 Packet Too Big error message.

[See [Configuring IPsec VPN on MX-SPC3 Services Card](#).]

- **Support for CMPv2 (MX240, MX480, and MX960 with MX-SPC3)**—Starting in Junos OS Release 21.3R1, Certificate Management Protocol version 2 is supported on MX-SPC3 service card.

[See [PKI Components In Junos OS](#).]

Additional Features

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

- **MACsec with GRES and NSR on MPC7E-10G line cards (MX480)**

[See [suspend-for](#) and [suspend-on-request](#).]

- **RADIUS over TLS (RADsec)**(MX5, MX10, MX40, MX80, MX104, MX150, MX204, MX240, MX480, MX960, MX2008, MX10003, MX10008, MX10016, and QFX5120-48YM)

[See [RADIUS over TLS](#).]

- **Stateless source Network Prefix Translation for IPv6 (NPTv6) packets** (MX Series routers with MPC10E and MX2K-MPC11E line cards.)

The NPTv6 translator translates the source address prefix in such a way that the transport layer checksum of the packet does not need to be recomputed.

[See [Stateless Source Network Prefix Translation for IPv6](#).]

- **Support for OAM on SRv6 and TI-LFA backup path over SRv6** (MX Series with MPC10E and MPC11E line cards) You can perform OAM operations on segment routing with IPv6 data plane (SRv6). We also support topology-independent loop-free alternate (TI-LFA) backup path for SRv6 in an IS-IS network on the MPCs.

[See [ping srv6](#) and [TI-LFA for SRv6](#).]

- **Support for VPLS over GRE tunnels** (MX Series routers with MPC10E line cards)

[See [Configuring Layer 2 Ethernet Services over GRE Tunnel Interfaces](#).]

- **Support for inline CCM, CFM, and scaling on MPC10E (MX240, MX480, MX960, MX2010, and MX2020) and MPC11E:**

- Inline CCM support on MPC10E and MPC11E.

- Support for CFM on MPC10E and MPC11E.
- In scaled mode, a CFM configuration can have 13,000 CCM sessions per MPC10E-10C-MRATE and MPC11E, and 26,000 for two (MPC10E-10C-MRATE, MPC10E-15C-MRATE, and MPC11E) line cards on the aggregated Ethernet interface.

[See [Inline Transmission Mode, Configuring Connectivity Fault Management \(CFM\)](#).]

- **TWAMP Light IPv6 addressing support** (ACX710, ACX2000, ACX2100, ACX5448, MX5, MX10, MX40, MX80, MX104, MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10008, MX10016, vMX, PTX1000, and PTX5000)

[See [Understand Two-Way Active Measurement Protocol on Routers](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.3R2](#) | 78
- [What's Changed in Release 21.3R1](#) | 80

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

What's Changed in Release 21.3R2

IN THIS SECTION

- [General Routing](#) | 79
- [Layer 2 Ethernet Services](#) | 79
- [Network Management and Monitoring](#) | 79
- [Routing Protocols](#) | 80

General Routing

- **Log messages are removed (MX Series)**—When PTP Aggregate Ethernet primary is configured, and PTP Aggregate Ethernet secondary is not configured, the log message "Profiles are being modified" is removed.
- **No support for PKI operational mode commands on the Junos Limited version (MX Series, PTX Series, and SRX Series devices)**—We do not support `request`, `show`, and `clear` PKI-related operational commands on the limited encryption Junos image ("Junos Limited"). If you try to execute PKI operational commands on a limited encryption Junos image, then an appropriate error message is displayed. The `pkid` process does not run on Junos Limited version image. Hence, the limited version does not support any PKI-related operation.

Layer 2 Ethernet Services

- **New output fields for subscriber management statistics (MX Series)**—If you enable the enhanced subscriber management, the non-DHCPv4 bootstrap protocol (BOOTP) requests might not get processed even if you configure the DHCP relay or server with the overrides `bootp-support` statement at the `edit forwarding-options dhcp-relay` hierarchy level. To monitor the DHCP transmit and receive packet counters, we've introduced the following output fields for `show system subscriber-management statistics dhcp extensive` operational command. - BOOTP boot request packets received - BOOTP boot reply packets received - BOOTP boot request packets transmitted - BOOTP boot reply packets transmitted

[See [show system subscriber-management statistics](#).]

Network Management and Monitoring

- **Change in behavior of SNMP MIB object `ifAlias`**—SNMP MIB object `ifAlias` now shows the configured interface alias. In earlier releases, `ifAlias` used to show configured interface description.
- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
 - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
 - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

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

Routing Protocols

- To achieve consistency among resource paths, the resource path `/mpls/signalling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counterip-addr='address'/state/countersname='name'/out-pkts/` is changed to `/mpls/signaling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counterip-addr='address'/state/countersname='name'/`. The leaf "out-pkts" is removed from the end of the path, and "signalling" is changed to "signaling" (with one "l").

What's Changed in Release 21.3R1

IN THIS SECTION

- [EVPN | 80](#)
- [General Routing | 80](#)
- [Junos XML API and Scripting | 81](#)
- [Layer 2 Ethernet Services | 82](#)
- [Network Management and Monitoring | 82](#)
- [Subscriber Access Management | 82](#)

EVPN

- **Support for displaying SVLBNH information**—You can now view shared VXLAN load balancing next hop (SVLBNH) information when you display the VXLAN tunnel endpoint information for a specified ESI and routing instance by using the `show ethernet-switching vxlan-tunnel-end-point esi esi-identifier esi-identifier instance instance svlbnh` command.

General Routing

- **Commit checks against incorrect configuration of SLC values (MX2020 and MX2010)**—We have introduced commit checks against incorrect configuration of sub line cards (SLCs). While configuring SLCs, if you specify any incorrect values (for example, unsupported Packet Forwarding Engine ranges,

CPU cores, or DRAM values), the configuration commit fails with an appropriate message to indicate the error.

[See [Configuring Sub Line Cards and Assigning Them to GNFs.](#)]

- **Enhancement to the show chassis pic command (Junos|Evo)**—You can now view additional information about the optics when you run the `<cli>show chassis pic </cli>` command. The output now displays the following additional field: MSA Version: Multi-source Agreements (MSA) version that the specified optics is compliant to. Values supported are: SFP+/SFP28 &-8212; SFF-8472 (versions 9.3 - 12.3), QSFP+/QSFP28 &-8212; SFF 8363 (versions 1.3 - 2.10), and QSFP-DD &-8212; CMIS 3.0, 4.0, 5.0. Previously, the show chassis pic command did not display this additional field.

[See [show chassis pic.](#)]

- **Enhancement to the show interfaces (Aggregated Ethernet) command (Junos|Evo)**—You can now view additional information about the MAC statistics when you run the `show interfaces extensive ae` command. The output now displays the following additional field: MAC statistics: Receive Transmit Broadcast packets 0 0 Multicast packets 0 0. Previously, the show interfaces extensive ae command did not display this additional field.

[See [show chassis pic.](#)]

- **Enhanced response to URR query or remove request (MX Series)**—When the control plane function sends a URR query or remove request, the Junos Multi-Access User Plane now sends the usage report in the modify response.
- **Support for multiple proxy-id list (MX5, MX10, MX40, MX80, MX104, MX240, MX480, MX960, MX2008, MX2010, and MX2020)**—MX Series routers does not support ID list except for the following two cases:
 - MX Series routers accept any-any traffic selector in proxy-id list from the remote device that supports ID lists.
 - MX Series routers accept the ID list if list can be reduced by removing duplicates to specific ID. For example, reduce ID list having 80.0.0.1 and 80.0.0.0/24 to super set ID 80.0.0.0/24.

```
list(any:0,ipv4(any:0-65535,0..3=80.0.0.1), ipv4_subnet(any:0-65535,0..7=80.0.0.0/24))
```
- **ISSU is not supported**—Unified in-service software upgrade (ISSU) is not supported when clock synchronization is configured for Precision Time Protocol (PTP) and Synchronous Ethernet.

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes

a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS.](#)]

Layer 2 Ethernet Services

- **Link selection support for DHCP**—We have introduced the `link-selection` statement at the `[edit forwarding-options dhcp-relay relay-option-82]` hierarchy level, which allows DHCP relay to add suboption 5 to option 82. Suboption 5 allows DHCP proxy clients and relay agents to request an IP address for a specific subnet from a specific IP address range and scope. Prior to this release, the DHCP relay dropped packets during the renewal DHCP process and the DHCP server used the leaf's address as a destination to acknowledge the DHCP renewal message.

[See [relay-option-82.](#)]

Network Management and Monitoring

- **Enhancement to the `snmp mib walk` command (PTX Series, QFX Series, EX Series, MX Series, SRX Series)**—The `ipv6IfOperStatus` field displays the current operational state of the interface. The `noIfIdentifier(3)` state indicates that no valid Interface Identifier is assigned to the interface. This state usually indicates that the link-local interface address failed Duplicate Address Detection. When you specify the 'Duplicate Address Detected' error flag on the interface, the new value (`noIfIdentifier(3)`) is displayed. Previously, the `snmp mib walk` command did not display the new value (`noIfIdentifier(3)`).
- **Changes in `contextEngineID` for SNMPv3 INFORMS (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Now the `contextEngineID` of SNMPv3 INFORMS is set to the local engine-id of Junos devices. In earlier releases, the `contextEngineID` of SNMPv3 INFORMS was set to remote engine-id.

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

- **Change in behavior of SNMP MIB object `ifAlias`**—SNMP MIB object `ifAlias` now shows the configured interface alias. In earlier releases, `ifAlias` used to show configured interface description.

Subscriber Access Management

- **PPPoE Active Discovery Network (PADN) deprecation (MX Series)**—We've deprecated the `padn` statement at the `[edit access domain map domain-map-name]` hierarchy level.

Known Limitations

IN THIS SECTION

- [General Routing | 83](#)
- [Infrastructure | 84](#)
- [MPLS | 84](#)
- [Network Management and Monitoring | 84](#)
- [Platform and Infrastructure | 85](#)
- [Routing Protocols | 85](#)

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

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

General Routing

- The ping latency behavior is expected for host generated ICMP traffic because of the Packet Forwarding Engine design queue polling the packets from ASIC. [PR1380145](#)
- The interface hold-down timer cannot be achieved for less than 15 seconds on the MPC11E line card. The interface on MPC11E might go down if the peer link goes down and downtime is less than 15 seconds. [PR1444516](#)
- MX-SyncE lock status shows LOCKED under the chassis synchronization extensive command when synchronization Ethernet source fails with the DUT configured with G.8275.1 profile. [PR1509356](#)
- Changing the scaled firewall profiles on the fly does not release the TCAM resources as expected. [PR1512242](#)
- LFM might flap during the MX Series Virtual Chassis ISSU. [PR1516744](#)
- Running "help apropos" command in configuration mode might generate a MGD core file. [PR1552191](#)
- On MX Series routers, unified ISSU or upgrade with validate option might fail if there is too less disk space in `/var/tmp/`. It is recommended to clear out all log files and core files before initiating upgrade

with validate option (that is, when you are not using no-validate option) or unified ISSU. It is better to clear all unwanted data using request system storage cleanup to cleanup all unwanted data. You must ensure there is at least 9 GB free space in **var/tmp** after copying vmhost package file to **/var/tmp/**. [PR1582554](#)

- When a packet, which triggers ARP resolution, hits services interface style filter on the output will have session create and close log with incorrect ingress interface. This typically occurs with the first session hitting such a filter. [PR1597864](#)
- Errors do not appear until there is a composite nexthop with two labels in the nexthop. This scenario must not appear and there is no impact in behavior. [PR1621689](#)

Infrastructure

- Image v-Vb7-2on fails with the following message: mgd core @ _rs_init, _rs_stir, _rs_stir_if_needed. [PR1568757](#)
- The Junos OS Release 21.1 and earlier are running FreeBSD version whereas from Junos OS Release 21.2 and later runs the FreeBSD 12. Upgrading to Junos OS release 21.2 or later from Junos OS Release 21.1 or earlier will mandatorily need configuration statement no-validate to be used during software image upgrade process. [PR1586481](#)

MPLS

- Rpd process might crash after network service configuration changed (example, range of MPLS labels) without rebooting all the Routing Engines (which is a system mandatory step). [PR1461468](#)

Network Management and Monitoring

- Configuring set system no-hidden-commands blocks/denies netconf/junoscript sessions. As a workaround, delete system no-hidden-commands configuration statement and start the netconf/junoscript sessions. [PR1590350](#)

Platform and Infrastructure

- MPC equipped with QX-chip might completely stop forwarding traffic after QX-chip internal memory error and MQChip DDRIF WO checksum error. [PR1197475](#)
- Below error logs are seen, while running `clear vpls mac-table`. [Mar 9 06:20:42.795 LOG: Err] `disp_force_callout(1994): EA[0:0].disp[0] forced callout timeout 0 msec`. [Mar 9 06:20:42.795 LOG: Err] `luss_send_callout_parcel(793): EA[0:0].disp[0] failed to send callout parcel (ptype 14, snum 977 tid 0)`. [Mar 9 06:20:43.510 LOG: Err] `dispatch_event_handler(684): EA[0:0].disp[0] PRIMARY_TIMEOUT (PPE 4 Zone 8)`. Impact: There will not be any functional impact during this issue, just the error logs. It occurs with a scaled count of more than 1.5L MACs and eventually all the MACs will get cleared successfully. [PR1575316](#)
- When deactivate services rpm and deactivate routing-options rpm-tracking commands are applied together and committed, some of the rpm tracked added routes are not deleted from the routing table. The issue cannot be seen when using the following steps:
 1. Issue the deactivate routing-options rpm-tracking command.
 2. Commit the configuration, then all the rpm tracked routes will be deleted.
 3. If the RPM service needs to be deactivated, issue the deactivate services rpm and commit.[PR1597190](#)

Routing Protocols

- If you do not issue the restart routing command after configuring the enhanced IP might result in a label inconsistency that causes the device to generate a rpd core file. [PR1577451](#)

Open Issues

IN THIS SECTION

- [EVPN | 86](#)
- [Flow-based and Packet-based Processing | 87](#)
- [Forwarding and Sampling | 87](#)
- [General Routing | 87](#)

- [Juniper Extension Toolkit \(JET\) | 92](#)
- [Layer 2 Ethernet Services | 92](#)
- [Layer 2 Features | 93](#)
- [MPLS | 93](#)
- [Network Management and Monitoring | 94](#)
- [Platform and Infrastructure | 94](#)
- [Routing Policy and Firewall Filters | 95](#)
- [Routing Protocols | 95](#)
- [Services Applications | 96](#)
- [Subscriber Access Management | 96](#)
- [User Interface and Configuration | 96](#)

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

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

EVPN

- A few duplicate packets might be seen in an AA EVPN scenario when the remote provider edge device sends a packet with an IM label due to MAC not learned on the remote PE device, but learned on the AA local PE device. The nondesignated forwarder sends the IM-labeled encapsulated packet to the PE-CE interface after MAC lookup instead of dropping the packet, which causes the duplicate packets to be seen on the customer edge side. [PR1245316](#)
- The vmcore process generates core file at `rts_ifbd_get_parent`, `rts_ifstate_chk_if_interesting_int`, `rts_ifstate_chk_if_interesting_int_with_stats`. [PR1542037](#)
- EVPN-MPLS multihoming control MACs are missing after VLAN ID removal and adding it back to a trunk logical interface of one of the multihoming PE devices. This is not a recommended way to modify VLAN ID configuration. Always perform symmetric change (remove or add VLAN ID) on both multihoming PE devices. [PR1596698](#)
- MAC IP moves across L2-DCI is not updated in MAC-IP table of the gateway nodes. This problem occurs only with the translation VNI when the MAC is moved from DC1 to DC2. VM moves across DC where there is no translate VNI configuration in the interconnect works as designed. [PR1610432](#)

Flow-based and Packet-based Processing

- Use 512 antireplay window size for IPv6 in fat-tunnel. The ESP sequence check might otherwise report out-of-order packets if the fat-tunnel parallel encryption is within 384 packets (12 cores * 32 packets in one batch). Hence there are no out-of-order packets with 512 antireplay window size.

[PR1470637](#)

Forwarding and Sampling

- fast-lookup-filter with match not supported in FLT hardware might cause the traffic drop. [PR1573350](#)

General Routing

- In MX104, you will see sporadic I2C error messages when Routing Engine CPU usage is high. The I2C might successfully access in the next polling with no impact. [PR1223979](#)
- On PTX Series routers with FPC-PTX-P1-A or FPC2-PTX-P1A, you might encounter a single event upset (SEU) event that might cause a linked-list corruption of the TQCHIP. [PR1254415](#)
- Next Generation Routing Engine (NG-RE) with RE-S-X6-64G, RE-S-2X00x6, and RE-PTX-X8-64G models on MX Series or PTX Series devices might encounter a transient system freeze of the Linux-based host (VM host) for about 20-35 seconds causing protocol flap, FPC restart that switches between the primary Routing Engines. [PR1312308](#)
- When you add VLAN as an action for changing the VLAN in both ingress and egress filters, the filter won't get installed. [PR1362609](#)
- With Next Generation Routing Engine (NG-RE), in some race conditions, the following messages might be seen on the primary Routing Engine: kernel: interrupt ACX7100-32C detected on "irq11:"; throttling interrupt source. [PR1386306](#)
- On MX series routers with MPC7E, MPC8E, or MPC9E installed, if optics QSFP-4X10GE-LR (Part number 740-054050) is used, the link might flap. [PR1436275](#)
- Primary PTP and secondary PTP port configuration accepts PTP packets with multicast MAC address according to the port settings. If you configure forwardable multicast, only PTP packets with forwardable MAC address are accepted, non-forwardable is dropped. If you configure link-local multicast, only PTP packets with non-forwardable MAC address are accepted, forwardable is dropped. [PR1442055](#)

- In race conditions, if a BGP route is resolved over the same prefix protocol next hop in a routing table that has routes of the prefix from different routing protocols, when the routes are flapping (firstly these routes are down and then up), the BGP route will be re-resolved, and then the rpd crash might be seen. [PR1458595](#)
- IP options router alert header is not hitting the firewall filter on egress. [PR1490967](#)
- When running `show pfe filter hw filter-name filter-name` command, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. [PR1495712](#)
- When backup Routing Engine stops, CB1 goes offline and comes back online. This restarts the backup Routing Engine, and it shows the reboot reason as "0x1:power cycle/failure". [PR1497592](#)
- A delay of 35 seconds is added in reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. [PR1514364](#)
- After performing unified ISSU on the Junos node slicing, the unsupported Field Replaceable Unit (FRU) unified ISSU will stay offline until it is brought online manually after the ISSU. This issue will cause a service or traffic impact for the offline FRUs. [PR1534225](#)
- FPC might generate a core file if flap-trap-monitor feature under `set protocols oam ethernet cfm performance-monitoring sla-iterator-profiles` is used and performance monitoring flap occurs. [PR1536417](#)
- "Socket to sflowd closed" error occur when the ukern socket to sflowd daemon (server) is closed. The error is rectified by itself as the client successfully reestablishes the connection in the subsequent attempts. When these errors are consistent, it indicates a communication issue between sflowd and the sFlow running on the FPC. [PR1538863](#)
- In scaled MX2020 router, with vrf localisation enabled, 4 million nexthop scale, 800k route scale. FPCs might go offline on GRES. Post GRES, router continues to report many fabric related CM_ALARMS. FPC might continue to reboot and not come online. Rebooting the primary and backup Routing Engine will help recover and the router gets stable. [PR1539305](#)
- PTP to PTP noise transfer is passing for impairments profile "400nsp-p_1Hz", but failing for profile "400nsp-p_0.1Hz" and lower BW profiles as well. The issue is common to 10g also. [PR1543982](#)
- 100G AOC from innolight does not come up after multiple reboots. It recovers after the interface is enabled or disabled. [PR1548525](#)
- This log is harmless Feb 27 20:26:40 xolo fpc3 Cannot scan phys_mem_size.out. Please collect `/var/log/*.out (0;0xdd3f6ea0;-1) (posix_interface_get_ram_size_info): Unknown error: -1.` [PR1548677](#)
- 5M DAC connected between QFX10002-60C and MX2010 does not link up. But with 1M and 3M DAC this interoperability works as expected. Also, it is to be noted 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 HW and SI teams and resolved. [PR1555955](#)

- VE and 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 or flood-group. Ideally, VE mesh-group does not require on a CE router where IGMP is enabled on CE interfaces. MX Series-based CE boxes have unlimited capacity of tokens, therefore this is not a major issue. [PR1560588](#)
- timingd-lc errors, "CdaExprClient: grpc api call ExprServerInfoGet failed" and "CdaExprClient: Failed to fetch server info error:5", seen on all fpcs after restarting router or fpc restart. [PR1561362](#)
- Because of the 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](#)
- Starting in Junos OS Release 21.1R1, Junos OS will be shipping with python3 (python2 is no longer supported). In ZTP process, if a python script is being downloaded, please ensure the python script follows python3 syntax (there are certain changes between python2 and python3 syntax). Also, until Junos OS Release 20.4R1, the python script had `#!/usr/bin/python` as the first line (that is, the path of the python interpreter). The same needs to be changed to `#!/usr/bin/python3` from Junos OS Release 21.1R1. [PR1565069](#)
- The chassisd logs are flooded with "pic_create_ifname: 0/0/0 pic type F050 not supported" messages for every port that is connected. This will happen every few seconds. [PR1566440](#)
- Stale TCNH entries are seen in new primary Routing Engine after switchover with NSR even though all the prpd routes are deleted. These TCNH entries are present because NSR is not supported for BGP static programmable routes. This leads to an extra reference count in the backup Routing Engine, due to which the next hop is not freed. [PR1566666](#)
- Packet Forwarding Engine error message "Tunnel id: does not exist" can be seen while executing `show dynamic-tunnel database statistics` after deactivating `routing-options dynamic-tunnel` when we have a high scale of tunnels. This is just a transient error message and has no functional impact. The error can appear while tunnels are getting deleted and will not be displayed after all the tunnels are deleted. [PR1568284](#)
- Copying files to `/tmp/` causes a huge `JTASK_SCHED_SLIP`. As a workaround, copy files to `/var/tmp/` instead. [PR1571214](#)
- Under very rare conditions for HA cluster deployment, when it does RGO failover and at same time, the control link is down, then it will hit this mib2d core file because the primary Routing Engine and secondary Routing Engine are out of syncing `dcd.snmp_ix` information. [PR1571677](#)

- On all Junos OS platforms, traffic loss might be observed because of a rare timing issue when performing frequent Interface Bridge Domain (IFBD) configuration modifications. This behavior is seen when the Packet Forwarding Engine receives out-of-order IFBD(s) from Routing Engine and might lead to the fxpc process crash and traffic drop. [PR1572305](#)
- The following messages might be seen in the logs from MPC11E line-card: Feb 9 11:35:27.357 router-re0-fpc8 aftd-trio[18040]: [Warn] AM : IPC handling - No handler found for type:27 subtype:9. As there is no functional impact, these logs can be ignored. [PR1573972](#)
- On MX Series routers, in a subscriber scenario with scaled around 32000 connections, the replication daemon might generate core files or stop running, which results in failure on subscriber services on the new Routing Engine after upgrading GRES. [PR1577085](#)
- In EVPN-VXLAN scenario with OSPF configured over the IRB, OSPF sessions might not get established due to connectivity issues. [PR1577183](#)
- This issue is caused by /8 pool with block size as 1, when the configuration 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](#)
- For input subscription paths containing a ":" character, the extension header in case of GNMI and certain fields for the show network-agent statistics CLI will have incorrect values. [PR1581659](#)
- On fully loaded devices, at times, firewall programming was failing due to scaled prefix configuration with more than 64800 entries. However, this issue is not observed in the development setup. [PR1581767](#)
- When the active secondary interface is deactivated, the PTP lock status is set to 'INITIALIZING' state in show ptp lock-status output for few seconds before BMCA chooses the next best slave interface. This is the day 1 behavior and there is no functional impact. [PR1585529](#)
- With preserve hierarchy configuration ON and option C is used with BGP CT, if the VPN CT stitching routes at ASBR are resolved over an SRTE tunnel with a single label, then the forwarding mpls.0 route programming will be incorrect on MX Series boxes. [PR1586636](#)
- In USF mode (MX-SPC3), NAT EIM mapping is getting created even for out to in FTP ALG child sessions. [PR1587849](#)
- On all Junos OS and EVO platforms, when there is a congestion on the link where telemetry streams are connected, then in a race conditions, there can be na-grpcd core and telemetry service will be impacted as na-grpcd will take a minute to come back online. [PR1587956](#)
- In USF mode (MX-SPC3), with NAPT44,EIM,APP and PCP configuration, show services session count on vms interface is not as expected for FTP traffic initiated from public side. [PR1588046](#)
- On all devices running Junos OS Release 19.1R3-S5-J3, the subscriber logical interface might get stuck after deleting the extensible subscriber services manager (ESSM). [PR1591603](#)

- In USF mode, for IPsec specific scenario involving GRES, RPD immediately purges the route entry (the ARI routes injected by IKED-based on negotiated traffic selector) as it considers it as a stale route entry on Routing Engine mastership switch which impacts the uplink (or encrypt) traffic until IKED adds back the ARI routes as part of the IKE and IPsec SA restore processing on mastership switch. In order to minimize the traffic loss, it is recommended to use the following configurable configuration statement: `set system services subscriber-management gres-route-flush-delay`. [PR1592655](#)
- On MX Series routers inline NPT does not translate source IPv6 of packet with authentication header present. The packet is simply passed through upstream. Consequently, it is not expected that downstream traffic arrives with NPT pool IPv6 address as IPv6 destination address and with authentication header. Such traffic might be malicious and this must be handled through external configuration. The fix suggested is to configure firewall for downstream direction that blocks traffic destined to NPT pool address and with authentication header. [PR1592957](#)
- Pim VxLAN does not work on TD3 chipsets enabling VxLAN flexflow after Junos OS Release 21.3R1. [PR1597276](#)
- On all MX Series routers, changing configuration AMS 1:1 warm-standby to load-balance or deterministic NAT might result in generating vmcore file and cause traffic loss. [PR1597386](#)
- MX2010, MX2020: MPC11E: Unified ISSU is not supported for software upgrades from Junos OS Releases 21.2 to 21.3 and Junos OS Releases 21.4 due to a flag day change. [PR1597728](#)
- On MX10008, MX10016, PTX10008, and PTX10016 with JNP10K-RE1, some of the SMART attributes of StorFly VSFBM8CC200G SSD might be shown as "Unknown_Attribute". There is no service impact due to this issue. [PR1598566](#)
- When PTP is on default profile and PTPoE is configured in stateful with ordinary clock-mode configuration is not supported. Below unsupported configuration does not throw commit error. There are no error logs reported with below unsupported configuration. Un-supported PTP configuration: `user@router# show protocols ptp clock-mode ordinary; stateful { interface xe-0/0/0.0 { multicast-mode { transport { ieee-802.3; } } } }` Stateful port configuration for PTP over Ethernet and default profile is supported only on boundary clock mode and not on ordinary clock mode. As a work around change the clock-mode or to remove stateful configuration. [PR1601843](#)
- When the interface transition occur from down to up, the carrier transition counter value of a particular interface can be incorrect when the peer interface takes longer time to come up. Configuring hold-time for up and down helps to resolve. [PR1601946](#)
- Comparing convergence time with Junos OS Release 21.1R1.5, seen degradation in ISISv6 , ospfv2 and ospfv3 convergence time. As it is a convergence time issue, many components will be involved and therefore need investigation from multiple teams (rpd, kernel, Packet Forwarding Engine). . [PR1602334](#)
- In an MX Series Virtual Chassis setup with MS-MPC or SPC3 service cards with AMS/MAMS interfaces configuration, it is possible that the traffic on an MPC2 line card in the protocol backup

chassis is not correctly load balanced due to timing conditions. As a workaround, reboot the affected line card while the service card is online. [PR1605284](#)

- In some NAPT44 and NAT64 scenarios, duplicate SESSION_CLOSE syslog will be seen. [PR1614358](#)
- With DSLite and NAT rule configuration to match ICMP and UDP traffic in place, ICMP error packet payload IP and UDP header translations are not happening properly. [PR1616633](#)
- Memory zone does not reflect appropriately while doing memory tests via Vty command test usp service-sets memory-testing start. [PR1619499](#)
- Enabling FIPS mode fails with self-test failure and kernel crash. [PR1623128](#)
- Zeroize RPC returns no positive reply. [PR1630167](#)
- DHCP ALQ syslog error bbesmgd[26939]: LIBSDB_RSMON_PS_TABLE_PTR_FAILURE: sdb_get_ps_interface_table_record:2076 failed to get the ps_table_header ptr. [PR1631858](#)
- On MX Series routers with SPC3 service card installed, TFTP control sessions are getting refreshed with inactivity time out after data session is closed, causing the control session to stay in session table for some more time. The service impact is minor or negligible as the TFTP control session will eventually get deleted after timeout. [PR1633709](#)
- After inserting local_dest_timeout, plane-1 is not going to check state. [PR1636943](#)

Juniper Extension Toolkit (JET)

- The jsd process might take sometime to detect abrupt termination of the socket at the collector or client side in certain cases. This can occur when flapping the interface on which the collector is connected to the router or when a firewall terminates the client port. In such cases, the client must wait for the connection termination to be detected, which could take around 1 hour, or restart the jsd process before being able to reconnect with the same client ID.

[PR1549044](#)

- The stub creation functions will not be available. [PR1580789](#)

Layer 2 Ethernet Services

- ZTP does not get activated after deleting the device once or twice. [PR1529246](#)

Layer 2 Features

- Adding one more subinterface logical interface to an existing interface causes 20-50 milliseconds traffic drop on the existing logical interface. [PR1367488](#)

MPLS

- BFD session flaps during unified ISSU only in MPC7E line card. The issue is not seen frequently. [PR1453705](#)
- The single hop BFD sessions might flap sometimes after GRES in a highly scaled setup which have RSVP link or link-node-protection bypass enabled. This happens because the RSVP neighbor goes down sometimes after GRES if RSVP hellos are not received before neighbor time out happens. As a result of the RSVP neighbor being down, RSVP installs a /32 route pointing to bypass tunnel which is required to signal backup LSPs. This route is removed when all LSPs stop using bypass after the link comes back. The presence of this /32 route causes BFD to flap. [PR1541814](#)
- The use-for-shortcut statement is meant to be used only in SR-TE tunnels which use Strict SPF Algo 1 (SSPF) prefix SIDs. If set protocols isis traffic-engineering family inet-mpls shortcuts and set protocols isis traffic-engineering tunnel-source-protocol spring-te is configured on a device, and if any SR-TE tunnel using Algo 0 prefix SIDs is configured with the use-for-shortcut statement, it could lead to routing loops or rpd process core files. [PR1578994](#)
- On the MX10008 and MX10016 routers, when there is scaled RSVP sessions (for example, 21,000) and the RSVP is enabled for all the interfaces, then the rpd process goes through all the interfaces which results into a high CPU utilization for some time. This also results in LSP flap. [PR1595853](#)
- When a protected link goes down, MPLS gets tunnel local repair message from RSVP and trigger CSPF computation. Next, MPLS gets link protection information through RRO notification. If MPLS receives TED notification first before RRO notification, then CSPF computation fails. Since the link protection flag is not set, MPLS thinks it is an unprotected link and brings down the LSP. [PR1598207](#)
- A few RSVP sessions are down in ingress nodes. [PR1631774](#)
- When RSVP setup protection is enabled, the LSP over a broadcast segment might stay down, due to a missing function of nexthop check for broadcast segment in code. [PR1638145](#)

Network Management and Monitoring

- When the ephemeral instance is deleted, physical files related to the instance is not deleted and the content of the file will remain as it is and might cause the device to behave uncertainly. [PR1553469](#)

Platform and Infrastructure

- The `commit synchronize` command fails because the kernel socket gets stuck. [PR1027898](#)
- Loss of traffic on switchover occurs when you use filter applied on the logical child interface. [PR1487937](#)
- On MX480 router, during the verification of GRES and NSR functionality with VXLAN feature, the convergence is not as expected L2-DOMAIN-TO-L3VXLAN. [PR1520626](#)
- When the DHCP relay mode is configured as no-snoop, the offer get dropped due to incorrect ASICs programming. This issue only affects while running DHCP relay on EVPN-VXLAN environment. [PR1530160](#)
- On the MX Series-based line card with firewall filter used scenario, in rare cases, adding and then deleting configurations at scale in multiple iterations might cause the line card to crash and FPC to restart. The traffic landing on this FPC is lost until it comes online again. [PR1589619](#)
- If authentication (for example, tacplus-server, radius-server) is configured on a device, it might fail to open files in a rare case, which might crash the mgd process. [PR1600615](#)
- Traffic loss of is observed with vrrp mastership change from backup to primary. This is seen while you bring up the route back after enabling the link. [PR1612504](#)
- With Junos OS Release 21.3R1, with EVPN VxLAN SMET multicast snooping configuration traffic might drop at VTEPs. [PR1613457](#)
- EX4400-48MP - VM core file is generated and Virtual Chassis split might be observed with multicast scale scenario. [PR1614145](#)
- On MX Series routers, during reboot, the aggregated Ethernet logical interfaces are first added, then deleted and again added. This flapping is a corner case where the filter attachment ipc has an older aggregated Ethernet logical interface index on which the filter bind fails. Filter will not be attached to the interface. Therefore, any filter related service will not work. [PR1614480](#)
- MAC addresses not learnt for some bridge domains. [PR1632411](#)
- Traffic drop is seen when you restart FPC of gre and aggregated Ethernet interface in L2GRE with virtual switch and aggregated Ethernet configured. [PR1640953](#)

Routing Policy and Firewall Filters

- Already configured routing-policies are incorrectly changed and all the configured "from" matching criterias are removed from them, when global default route-filter walkup option is changed, that is, when add/delete of set policy-options default route-filter walkup configuration is performed. This issue affects only those routing policies which do not have "from route-filter" configured in any of the terms. [PR1646603](#)

Routing Protocols

- When interoperating with other vendors in a draft-rosen multicast VPN, by default the Junos OS attaches a route target to multicast distribution tree (MDT) subsequent address family identifier (SAFI) network layer reachability information (NLRI) route advertisements. But some vendors do not support attaching route targets to the MDT-SAFI route advertisements. In this case, the MDT-SAFI route advertisement without route-target extended communities will be excluded from propagating if the BGP route target filtering is enabled on a device running Junos OS. Note that draft-rosen-idr-rtc-no-rt has been created in IETF to document this issue and carry the proposed fix through standards. [PR993870](#)
- TILFA backup path fails to install in LAN scenario and also breaks SR-MPLS TILFA for LAN with more than four end-x SIDs configured per interface. [PR1512174](#)
- Conformance issues with draft-ietf-idr-bgp-ext-opt-param. In previous versions of RFC 9072 (that is, draft-ietf-idr-bgp-ext-opt-param), the required optional-parameter length is 255 in order to trigger the updated behavior. Later editions of the internet draft permitted non-zero optional parameter length values to be used. [PR1554639](#)
- clns ping statement fails through L3 VPN. [PR1559005](#)
- In a Virtual Chassis or Virtual Chassis fabric scenario, inconsistent MCSNOOPD core file is seen when the igmp-snooping configuration is removed. [PR1569436](#)
- SHA-1 system login password format are not accepted post the upgrade. [PR1571179](#)
- On all platforms supporting unified ISSU, if ISSU is performed on two routers connected over Link Fault Management (LFM), the process is aborted with 'Aborting Daemon Prepare' on one of the routers. The bidirectional forwarding detection (BFD) process get stuck at abort state and is not reverted back to idle state. Any subsequent attempt of ISSU on failed node fails with the same message. [PR1598786](#)
- When MPLS traffic-engineering and rib inet.3 protect core configuration statement is enabled then transport routes in inet.3 will not be used for route resolution. [PR1605247](#)

Services Applications

- DTCP radius-flow-tap fails to program Packet Forwarding Engine when trigger X-NAS-Port-Id exceeds 48 character length. [PR1647179](#)

Subscriber Access Management

- Event-timestamp in RADIUS Acct-Stop might show future time in certain circumstance. [PR1643316](#)

User Interface and Configuration

- bbe-smgd core file is observed 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](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 97](#)
- [Resolved Issues: 21.3R1 | 113](#)

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

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

Resolved Issues: 21.3R2

IN THIS SECTION

- Application Layer Gateways (ALGs) | 97
- Class of Service (CoS) | 98
- EVPN | 98
- Flow-based and Packet-based Processing | 98
- Forwarding and Sampling | 98
- General Routing | 99
- High Availability (HA) and Resiliency | 106
- Infrastructure | 107
- Interfaces and Chassis | 107
- Layer 2 Ethernet Services | 107
- MPLS | 108
- Multicast | 109
- Network Management and Monitoring | 109
- Platform and Infrastructure | 109
- Routing Policy and Firewall Filters | 110
- Routing Protocols | 110
- Services Applications | 111
- Subscriber Access Management | 112
- User Interface and Configuration | 112
- VPNs | 112

Application Layer Gateways (ALGs)

- On MX Series routers, the flowd daemon will crash if the SIP ALG is enabled and specific SIP messages are processed (CVE-2022-22175). [PR1604123](#)
- Junos OS: Flowd core file is generated if the SIP ALG is enabled and a specific session initiation protocol (SIP) packet is received (CVE-2022-22178). [PR1615438](#)

Class of Service (CoS)

- Transit packets from local to remote VTEP might get punted to CPU and cause DDoS events. [PR1489233](#)
- In a Junos Fusion deployment, dynamically removing and adding a logical interface under interface-set might lead to traffic control profile on the interface-set not working. [PR1593058](#)
- The fabric queues priority might not get changed after activating or deactivating CoS configuration. [PR1613541](#)

EVPN

- Baseline EVPN-VXLAN transition from IPv4 to IPv6 or vice versa does not work in certain sequence. [PR1552498](#)
- The BUM traffic might be dropped after changing any configuration on the device without router-id configured. [PR1576943](#)
- Bridge mac-table learning entries might not be as expected for the EVPN-MPLS routing instance. [PR1600310](#)
- Missing MAC address entries in EVPN mac-table despite the presence of the corresponding Type 2 route. [PR1611618](#)
- Few ARP/ND/MAC entries for VLANs are missing with MAC-VRF configuration. [PR1609322](#)
- The l2ald crash might be seen after performing restart routing on EVPN PE. [PR1629426](#)
- Removing the configuration statement `es-label-oldstyle` might not be committed if it is the only statement configured under the EVPN protocol. [PR1629953](#)
- The traffic loss might be seen when the link goes down for the local ESI. [PR1632723](#)

Flow-based and Packet-based Processing

- Bad file descriptor is observed when descriptive `clear services inline-monitoring statistics` statement is performed. [PR1624094](#)

Forwarding and Sampling

- More than 5 minutes delay in getting the response for the `clear interfaces statistics all` command with RIB scale configuration. [PR1605544](#)
- Commit is allowed even if firewall filter is not applied to the FPC. [PR1618231](#)

- The FPC might crash when an interface participating in "next-interface" filter action flap. [PR1622585](#)
- BFD session on a few aggregated Ethernet stuck in init/down with slice 2 connections in GNF. [PR1625309](#)

General Routing

- DHCP subscribers might not be synchronized to backup BNG when DHCP ALQ is configured without topology-discover. [PR1620544](#)
- On MX10003, despite of having all AC low or high PEM, **Mix of AC PEMs** alarm is raised. [PR1315577](#)
- Error message **sensord: Error updating RRD file: /var/run/sensord.rrd** might be seen on WRL9-based line card. [PR1420927](#)
- The following error messages are observed **unable to set line-side lane config (err 30)**. [PR1492162](#)
- During flooding, MAC is learnt only on normal access port but not on the aggregated Ethernet interface trunk port. [PR1506403](#)
- Next-hops are not programmed correctly after Virtual Chassis global switchover. [PR1518467](#)
- Junos OS 'et-' interface get stuck and remains down between two particular ports. [PR1535078](#)
- Some transmitting packets might get dropped because the "disable-pfe" action is not invoked when the fabric self-ping failure is detected. [PR1558899](#)
- Na-grpcd process might generate a core file during longevity tests. [PR1565255](#)
- When using log templates (introduced in Junos OS Release 21.1R1) with unified policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile set security log profile *name* default-profile, that can be used to improve this behaviour when multiple log profiles are defined. [PR1570105](#)
- Interfaces might fail to come up on MX240, MX480 and MX960 platforms [PR1571274](#)
- pkid core file is generated at #0 0x08456bb3 in je_bitmap_set (bitmap=0x8c7c00c, binfo= optimized out, bit= optimized out) at ../../../../../../src/external/bsd/jemalloc/dist/include/jemalloc/internal/bitmap.h:101. [PR1573892](#)
- **CHASSISD_FRU_IPC_WRITE_ERROR: fru_send_msg: FRU GNF 2, errno 40, Message too long** might appear periodically in the chassisd logs. [PR1576173](#)
- MIC specific alarms are not cleared after MIC reboot. [PR1576370](#)

- MPC7E, MPC10E, MX-SPC3 and LC2103 line cards might become offline when the device is running on FIPS mode. [PR1576577](#)
- The subscribers over PS interface are not cleared after FPC offline. [PR1580812](#)
- The deleted loopback route prefix might exist under subscriber management when the loopback IP is deleted and added in a single commit. [PR1582263](#)
- The line cards might fail after hitting the I2C error on MX Series router FPC. [PR1583060](#)
- A high rate of small packets might cause CPU hogging and firmware crash in MPC5E and MPC6E cards. [PR1587551](#)
- PEM capacity shows incorrectly on MX10003 platform. [PR1587694](#)
- Fabric link training might be seen if fabric self ping silently drop or get discarded. [PR1590054](#)
- Some logical interfaces might go down under logical tunnel because of the limited number of MAC addresses in a pool. [PR1591853](#)
- The DCI interVNI and intraVNI traffic might silently drop or get discarded in gateway node due to the tagged underlay interfaces. [PR1596462](#)
- Mscsnoopd might crash during deleting and then adding layer-2 forwarding configuration after performing a unified ISSU. [PR1596483](#)
- The l2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable. [PR1599094](#)
- Traffic might be silently dropped and discarded upon link flap after a topology change. [PR1599215](#)
- NSR switchover performed with BGP SR-TE tunnels might generate an rpd core file. [PR1599446](#)
- High FPC CPU utilization might be intermittently observed after receiving a great number of NS/NA message. [PR1600318](#)
- gNMI telemetry might stop working after the Routing Engine switchover. [PR1600412](#)
- Traffic might be dropped at NAT gateway if EIM is enabled. [PR1601890](#)
- Kernel crash might be seen when static routes are configured with GRE interfaces being used as next hop. [PR1601996](#)
- Some EVPN mac-ip entries might get stuck and do not age-out. [PR1602010](#)
- In a rare case, the l2ald core file is seen when EVPN (mac-vrf) uses IPv4 underlay. [PR1602244](#)
- Junos OS: Specific packets over VXLAN cause FPC memory leak and ultimately reset (CVE-2022-22170). [PR1602407](#)

- IPv6 link local BFD session might not come up if you do not have a child link of an aggregated Ethernet mapped to Packet Forwarding Engine inst 0. [PR1602493](#)
- Jflow-syslog for CGNAT might use 0x0000 in IPv4 identification field for all fragments. [PR1602528](#)
- The statement `show system errors fru detail` does not display **reset-pfe** as the `cmerror` configured action. [PR1602726](#)
- When using J-Web with HTTP an attacker might retrieve encryption keys via person-in-the-middle attacks (CVE-2021-31386). [PR1603199](#)
- Packet loss might be seen on filter-based GRE deployments. [PR1603453](#)
- Traffic loss might be seen on the device because of the continuous errors observed in the Fabric Healing process (FHP) phase-1. [PR1603499](#)
- 21.3TOT:TCP_TLS_SYSLOG:core-usf-qnc-a-fpc3.pic1-flowd_spc3.elf.0.tgz is seeing while verifying TCP-based logging functionality with GRES with AMS-nexthop style. [PR1603466](#)
- NSSU performed with MACsec configuration might result in `fxpc` core file. [PR1603602](#)
- VRRP and BFD might flap on the IRB interface on MPC10 and MPC11 line cards. [PR1604150](#)
- NPC logs are seen when VRF localisation is enabled. [PR1604304](#)
- GRE tunnel might flap when hierarchical-scheduling is configured. [PR1605189](#)
- The interface on MCP3-NG HQoS or MPC7E flaps continuously after enabling LACP on aggregated Ethernet interface. [PR1605446](#)
- VM host platforms might boot exactly 30 minutes after executing `request vmhost halt` command. [PR1605971](#)
- 5G-CUPS:bbe-cups-5G-setup:wf-eabu-dev.tadcaster:re1 {version} vmcore.0.gz. [PR1606146](#)
- Fabric error might be seen when MPC10E to MPC2, MPC3, MPC4, MPC5, and MPC6 based FPC fabric traffic is congested. [PR1606296](#)
- Observing continuous SNMP trap for "Over Temperature!" for all the Renault_Daniel line cards (FPC: JNP10K-LC480). [PR1606555](#)
- Random IP assignment might be done on MX Series routers configured with PCP and DS-Lite. [PR1606687](#)
- New subscribers might not connect due to the CR-features service object missing on FPC. [PR1607056](#)
- IPv6 link-local BFD session might not come up on MX Series routers. [PR1607077](#)

- TCP traffic might be dropped on source port range 512 to 767 when the FlowSpec IPv6 filter is configured. [PR1607185](#)
- Commit related to dynamic profile configuration changes might fail upon executing request `vmhost reboot routing-engine` both on MX Series routers. [PR1607494](#)
- The speed auto-negotiated SFP-T transceiver might not be joined to the aggregated Ethernet after performing `dcd restart` or Routing Engine switchover on MX104. [PR1607734](#)
- MPC10 and MPC11 filters matching unknown-unicast does not take effect. [PR1608723](#)
- The FPC might crash when the option `sensor-based-stats` is configured. [PR1608871](#)
- BFD over GRE tunnel interface stuck in "init" state with GRES enabled. [PR1609630](#)
- DHCP subscribers over PWHT might be dropped upon GRES after the system reboot. [PR1609818](#)
- The single-vlan tagged subscribers might fail to reconnect through dynamic-vlan over PS interface. [PR1609844](#)
- Interface flaps might be observed on certain ports. [PR1609988](#)
- The `authd` process and RADIUS might have stale L2BSA subscriber entries [PR1610476](#)
- Traffic loss might be observed if `dot1X` is configured with supplicant `multiple` and authenticated user from RADIUS is in single supplicant mode. [PR1610746](#)
- MACsec session might be dropped because of one way congestion. [PR1611091](#)
- Erratic behaviour might be seen on the platforms using MPC line cards after unified ISSU is performed. [PR1611165](#)
- Inter-vlan connectivity might be lost in an EVPN-VXLAN with CRB topology. [PR1611488](#)
- The service PICs are unable to come up when `dnsmf` package is configured. [PR1612316](#)
- The routing protocol engine CPU is getting stuck at 100 percent. [PR1612387](#)
- The B4 client traffic will be dropped on MX-SPC3 based AFTR in DS-Lite with EIM activated CGNAT scenario. [PR1612555](#)
- Some of the fabric links might go into faulty state after swapping FPC LC1201 with LC1202. [PR1612624](#)
- `l2ald` core file is generated during routing-instance configuration change. [PR1612738](#)
- The PFE/SIB/SCBE/FPCs might reboot due to the unexpected fabric errors shown on MX240, MX480, and MX960 platforms. [PR1612957](#)

- Memory might be exhausted when both BGP rib-sharding and the BGP Optimal Route Reflection (ORR) is enabled. [PR1613104](#)
- Traffic loss might be observed because of the shaping rate being incorrectly adjusted in a subscriber environment on MX Series routers. [PR1613126](#)
- Enhanced-hash-key might not take effect when configured with forwarding-options. [PR1613142](#)
- IGP routing updates might be delayed to program in Packet Forwarding Engine after interface flaps in a scaled BGP routes environment. [PR1613160](#)
- Enabling security-metadata-streaming DNS policy might cause a dataplane memory leak. [PR1613489](#)
- The rpd process might crash in BGP rib-sharding scenario. [PR1613723](#)
- Any irrelevant configuration changes might trigger NAT routes flap on MX Series routers in USF mode. [PR1614688](#)
- Modifying the input service-filter via COA might fail in subscriber management environment. [PR1614903](#)
- Line-cards might be unstable because of the continuous growing memory usage of evo-cda-bt app. [PR1614952](#)
- Export memory and temperature metrics for all existing components when it subscribes to telemetry sensor. [PR1615045](#)
- The l2ald process might crash in an EVPN scenario. [PR1615269](#)
- Traffic drop may occur when huge number of EIM mappings are created or deleted continuously. [PR1615332](#)
- Request to provide an API which lists the potential policy given in a session id. [PR1615355](#)
- The rasdaemon processes memory leak triggered by hardware memory errors on the VMHost platforms. [PR1615488](#)
- Slow memory leak (32 bytes each time) of rpd might be seen. [PR1616065](#)
- show subscribers accounting-statistics, show services l2tp session interface asi0.xx statistics might not work on LNS with ASI interfaces. [PR1616454](#)
- The dual Routing Engine system might not be GRES ready after backup Routing Engine reboot in a subscriber management environment. [PR1616611](#)
- L2 cpd memory leak might lead l2cpd process to crash. [PR1617151](#)
- In MX Series VC spcd running on SPC3 crashes. [PR1617280](#)

- MPC8E in 1.6T bandwidth mode might not work correctly. [PR1617469](#)
- The l2cpd core file is seen with FIP snooping configuration on any interface. [PR1617632](#)
- Traceroute packets might get dropped in SFW service-set when other service-sets with asymmetric traffic processing are also enabled on the same MS-MIC/MS-MPC. [PR1617830](#)
- GMC clock class is seen transmitted for an additional 16 seconds after the PTP source switches from one line card to another. [PR1618344](#)
- The traffic loss might be seen after cleaning the large-scaled NAT sessions in MS-SPC3 based Next-Gen services inter-chassis stateful high availability scenario. [PR1618360](#)
- A device which is configured IP interface(ip-x/x/x) cannot send encapsulated IPv4-over-IPv6 packets to a remote device in case of transit packets. [PR1618391](#)
- The clksyncd might crash and PTP/SyncE might not work. [PR1618929](#)
- Support whole (atomic) updates at CNHG level. [PR1619011](#)
- The nsd might crash while validating NAT translation on MX Series routers with SPC3. [PR1619216](#)
- Traffic might be dropped when RSVP is configured with mtu-signaling. [PR1619510](#)
- Additional commit warnings and errors were introduced to improve security log profile usability. [PR1619694](#)
- The bbe subscriber access services might get stuck during rebooting the one redundancy line-card of the RLT. [PR1620227](#)
- Observed output drop packet while verifying services PCEF subscribers. [PR1620421](#)
- OAM CFM session does not come up if ERPS configured and CFM control traffic uses the same VLAN as ERPS control traffic. [PR1620536](#)
- High wired memory utilization might be observed if GRES is enabled. [PR1620599](#)
- EVPN type 5 routes might not be installed. [PR1620808](#)
- Static-subscribers session might get stuck in initializing state after ungraceful Routing Engine switchover. [PR1620827](#)
- CoS hierarchy for logical interface missed in backup leg after rebooting FPC when we have subscriber logical interface targeting over IFLSET non-targeting. [PR1621164](#)
- Flapping of all ports in the same Packet Forwarding Engine might cause Packet Forwarding Engine to be disabled. [PR1621286](#)
- Commit failure while applying tunnel interface configurations using openconfig CLI. [PR1621369](#)

- Traffic loss is seen on the new primary Routing Engine post GRES. [PR1621696](#)
- When PHY-Sync state moved to 'False' it internally disables the PHY-timestamping of PTP packets. [PR1622108](#)
- Invocation of netconf get command will fail if there are no L2 interfaces in the system. [PR1622496](#)
- Port speed might show as 100G even though chassis configuration is set for 40G manually. [PR1623237](#)
- The chassisd memory leak might be seen after adding or removing an interface configuration. [PR1623273](#)
- The aggregated Ethernet member link might not be correctly populated on the Packet Forwarding Engine after FPC restart on MX Series platforms. [PR1624772](#)
- On single IPSec tunnel with PMI sending an internet traffic packet processing might get delayed due to session management issue. [PR1624974](#)
- Junos OS: Specific packets over VXLAN might reset FPC(CVE-2022-22171). [PR1625292](#)
- The bbe-statsd crash might be seen in the LTS subscriber scenario. [PR1625648](#)
- gNMI set RPC might fail when multiple values within a single gNMI SetRequest are used for the Junos telemetry interface. [PR1625806](#)
- Packet loops in the PIC even after stopping the traffic on MX Series routers with SPC3 line card. [PR1625888](#)
- The bbe-smgd might crash on the backup Routing Engine after unified ISSU or GRES. [PR1626091](#)
- Some interfaces might not come online after linecard reboots. [PR1626130](#)
- Implement show task scheduler-slip-history to display no of scheduler slips and last 64 slip details. [PR1626148](#)
- The chassisd might crash on MX104. [PR1626486](#)
- The autoconf might not work if the DHCPv4 discover message has an option-80 (rapid commit) ahead of option-82. [PR1626558](#)
- Memory leak might occur in the pfd process when the statement flat-file-profile is configured with the use-fc-ingress-stats statement. [PR1628139](#)
- EAPoL packets over l2circuit may get dropped at the tunnel start. [PR1628196](#)
- Broadcast traffic might not be forwarded to LT interface in VPLS routing instance after LT interface is deleted then added back. [PR1626714](#)

- The line card might crash and reload if the EVPN MAC entry is not deleted correctly. [PR1627617](#)
- show system subscriber-management route summary does not report route summary as expected. [PR1629450](#)
- The l2ald might be stuck in "issu state" when ISSU is aborted [PR1629678](#)
- Multiple link flaps and traffic might be lost on the links. [PR1630006](#)
- The kmd daemon might crash with core file every few minutes on the MX Series routers. [PR1630070](#)
- LLDP packets might be sent with incorrect source MAC for RETH/LAG child members. [PR1630886](#)
- The kmd might crash since the pkid requested memory leak happens on MX Series platforms. [PR1631443](#)
- RPD core file is generated on RE1 `krt_inh.c,krt_nexthop.c,krt_remnant.c`. [PR1631871](#)
- When deleting the VNI and there is another vlan-id-list with a different VNI might cause traffic loss. [PR1632444](#)
- The bbe-smgd process might crash after removing and adding a child link from aggregated Ethernet interface. [PR1633392](#)
- Slow chassis memory leak may occur when chassisd related configuration change is committed. [PR1634164](#)
- PTP clock class is incorrectly downgraded to 248 when PTP is enabled on MIC linecard which does not support phy-timestamping. [PR1634569](#)
- Data might not be exchanged via EVPN-VxLAN domain. [PR1635347](#)
- SFP-1FE-FX might not function properly on MIC-MACSEC-20G. [PR1636322](#)
- Delay might be observed for the interfaces to come up after reboot/transceiver replacement. [PR1638045](#)
- When all configured anchor Packet Forwarding Engines are offline on the SAEGW-u, there might be a peer association mis-match between the SAEGW-u and SAEGW-c. [PR1634966](#)
- CFM CCM PDU is not forwarded transparently on generating a core file if the physical interface is configured under OAM protocol. [PR1635293](#)
- Locally switched traffic might be dropped on MX10003 with ESI configured. [PR1638386](#)

High Availability (HA) and Resiliency

- Memory leaking might occur on the backup Routing Engine when ksyncd is in inconsistent state and has encountered an initialization error. [PR1601960](#)

- When MTU is configured on an interface a rare ifstate timing issue occurs at a later point resulting in ksyncd process crash on backup Routing Engine. [PR1606779](#)

Infrastructure

- The fxpc process might crash and generate a core file. [PR1611480](#)

Interfaces and Chassis

- The dcd process crash might be observed after removing the aggregated Ethernet logical interface from the targeted distribution database. [PR1591032](#)
- lo0 family maximum labels is non-adjustable in syslog messages. [PR1611098](#)
- Commit check failure might occur if similar interfaces are configured under VRRP group. [PR1617020](#)
- Delay in application of CLI configuration by DCD when an aggregated Ethernet interface members are configured via JET API. [PR1621482](#)
- CFM enhanced SLA iterators monitoring might stop after restarting chassis-control daemon in vMX. [PR1622081](#)
- The subscribers might be deleted when "host-prefix-only" statement is configured on the underlying interface in GRES scenario. [PR1630229](#)
- The syslog messages and the dcd crash might be seen in Junos OS. [PR1633339](#)
- VRRP route tracking for routes in VRF might not work if "chained-composite-next-hop ingress l3vpn" is used. [PR1635351](#)
- Some daemons might get stuck when snmpd is at 100 percent CPU utilization. [PR1636093](#)
- FPC might crash if the continuity-check interval under CFM is modified. [PR1636226](#)
- On Junos OS Release 20.3 and later, the tracking routes of VRRP might become unknown after upgradation. [PR1639242](#)

Layer 2 Ethernet Services

- Making configuration changes with apply-group add/delete associated with DHCP may result in client connection failure. [PR1550628](#)
- The jdncpd process might crash under certain conditions. [PR1603992](#)
- DHCP leasequery is failing to restore binding when the reply is received over IRB interface. [PR1611111](#)

- Enabling DHCP on Junos OS platforms might cause the router's file system storage to get filled up with log files. [PR1617695](#)
- The jdhcpcd crashes upon receiving a specific DHCP packet (CVE-2022-22179). [PR1618977](#)
- Circuit-id handled incorrectly with backup node for ALQ with topology discover configured. [PR1620461](#)
- The jdhcpcd process crashes in DHCP/DHCPv6 environment. [PR1625011](#)
- The jdhcpcd process may stuck at 100 percent post clients login/logout. [PR1625112](#)
- Option-82 might not be attached on DHCP request packets. [PR1625604](#)
- The rpd scheduler might continuously slip after GRES when there are 7000 DHCP clients in a subscriber management environment. [PR1625617](#)
- Non-DHCPv4 BOOTP protocol packets might not be processed if enhanced subscriber management is enabled. [PR1629172](#)

MPLS

- D-CSPF node segment label: unresolved when node index 0 is configured. [PR1564169](#)
- Post GRES, LDP P2MP traffic might be interrupted. [PR1609559](#)
- RPD might crash on standby_re LDP module when VPLS mac-flush enabled on peer by default or configuration. [PR1610638](#)
- LDP does not support policy import with rib-groups. [PR1611081](#)
- The rpd process might crash if express segments using SR-TE underlay are configured. [PR1613372](#)
- The rpd core file might be generated for few value configurations of signaling bandwidth on container LSP. [PR1614248](#)
- Protected LSP goes down with strict hops and link protection configured. [PR1616841](#)
- LDP protections paths might not be established when auto-targeted-session statement is deactivated and activated. [PR1620262](#)
- VCCV BFD session keeps flapping between MX Series and peer device if ultimate-hop popping is enabled. [PR1634632](#)
- The rpd memory leak may be observed in a subscriber management environment with RSVP. [PR1637645](#)
- Dynamic bypass LSP might flap at every re-optimization interval. [PR1639292](#)

Multicast

- Intermittent p2mp traffic drop might be seen in MVPN scenario [PR1608311](#)

Network Management and Monitoring

- Ephemeral instance configuration not removed even after deleting the ephemeral instance from set system configuration-database. [PR1553469](#)
- Master-eventd process might go down when syslog configuration is misconfigured. [PR1611885](#)
- Syslog messages may be lost partially in case of lots of messages generated to eventd. [PR1612535](#)
- After receiving a specific number of crafted packets snmpd will segmentation fault (SIGSEGV) requiring a manual restart (CVE-2022-22177). [PR1613874](#)

Platform and Infrastructure

- The subscribers might not come online after interface flaps on MX Series platforms. [PR1591905](#)
- "XMCHIP_CMERROR_PT_INT_REG_PCT_PAR_ERR (0x70296)" might be observed on MPC5 card which triggers Packet Forwarding Engine disable. [PR1597953](#)
- Traffic through one SPU may stop with potential packet drop issue with alarm as FPC Major Errors raised due to the PIC_CMERROR_TALUS_PKT_LOSS error. [PR1600216](#)
- On MX Series routers, mbuf corrupts resulting in generating a vmcore file on both the Routing Engines. [PR1602442](#)
- The FPC might crash if flow-table-size is configured on MX Series routers. [PR1606731](#)
- Multicast traffic is dropped when forwarded over VPLS via IRB. [PR1607311](#)
- FPC crash might be seen due to mac-move between two interfaces under same bridge domain. [PR1607767](#)
- Degraded traffic processing performance might be observed in case of processing high PPS rate traffic. [PR1619111](#)
- CoS custom classifier might not work on the logical interface. [PR1619630](#)
- MX Series-based line cards might crash when PFE memory is hot-banking. [PR1626041](#)
- Unrealistic service accounting statistics might be reported due to firewall counter corruption. [PR1627908](#)

- Error message "gencfg_cfg_msg_gen_handler drop" is seen after running commit command. [PR1629647](#)
- The packet drop might be seen on FPC on MX Series-based platforms. [PR1631313](#)
- Committing authentication-key-chains statement under groups might fail. [PR1626400](#)
- Continuous fabric link sanity check interrupts in intervals of weeks might cause at some point fabric input block traffic getting dropped or discarded. [PR1636060](#)

Routing Policy and Firewall Filters

- The interface-routes rib-group policy does not work as expected in the VxLAN scenario. [PR1537306](#)
- Evaluation of inet-vpn route-filters might not work with /32 exact statements for BGP flowspec routes. [PR1618726](#)

Routing Protocols

- New version of OpenSSL (1.1.1) is not supported for NTF-agent of Junos telemetry interface. [PR1597714](#)
- Observing commit error while configuring "routing-options rib inet6.0 static" on all Junos OS platforms. [PR1599273](#)
- The rpd core file might be observed due to memory corruption. [PR1599751](#)
- Kernel crash might be observed on platforms having BGP configured with family L2VPN. [PR1600599](#)
- rpd crash might be seen after deactivating and then activating the interfaces [PR1605620](#)
- The BGP replication might be stuck in "InProgress" state. [PR1606420](#)
- Multicast traffic might be duplicated on subscriber interface on MX Series routers. [PR1607493](#)
- The rpd crash might be seen with telemetry used setup. [PR1607667](#)
- microloop-avoidance post-convergence-path might not work without source-packet-routing. [PR1608992](#)
- The rpd might crash after a commit if there are more than one address in the same address ranges configured under 'bgp allow'. [PR1611070](#)
- The interface might receive multicast traffic from a multicast group which it is not interested in. [PR1612279](#)
- The rpd crash might be seen on all Junos OS platforms [PR1613384](#)

- Undesired protection path may get selected for some destination prefixes [PR1614683](#)
- The memory leak on rpd might be observed after running "show route" CLI command. [PR1615162](#)
- BFD sessions flapping may occur after performing GRES. [PR1615503](#)
- The wrong BGP path may get selected even when a better/preferred route is available. [PR1616595](#)
- Traffic drop will be seen when VPN labels are incorrectly allocated due to change in nexthop. [PR1617691](#)
- Verification of BGP peer count fails after deleting BGP neighbors. [PR1618103](#)
- Junos OS: OpenSSL Security Advisory [24 Aug 2021.] [PR1618985](#)
- The rpd might crash and restart when NSR is enabled. [PR1620463](#)
- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific BGP export policies. [PR1626367](#)
- Multipath route with List-NH which has Indirect-NH as members fails into BGP-LU. [PR1626756](#)
- The contributing routes might not be advertised properly if "from aggregate-contributor" is used. [PR1629437](#)
- The multicast forwarding cache might not get updated after deactivating the scope-policy configuration. [PR1630144](#)
- The BGP ECMP might not work and multipath route wont be created. [PR1630220](#)
- The rpd might crash after clearing isis database. [PR1631738](#)
- The BGP session might flap after rpd crash with switchover-on-routing-crash and NSR enabled in a highly scaled environment. [PR1632132](#)
- IS-IS database may not be synchronized in some multiple areas scenario. [PR1633858](#)
- Multipath route getting formed for a VPN prefix due to incorrect BGP route selection logic. [PR1635009](#)

Services Applications

- L2TP tunnels might go down and not able to re-establish after restarting the bbe-smgd process. [PR1629104](#)
- Tunneled subscribers may be stuck in terminating state in L2TP subscriber scenario. [PR1630150](#)

Subscriber Access Management

- Install discard routes is not supported on APM managed BNGs running Junos OS Release 21.3R1. [PR1604967](#)
- Prefix duplication errors might occur for DHCPv6 over PPPoE subscribers. [PR1609403](#)
- DHCP session fails with the configuration statement `session-limit-per-username`. [PR1612196](#)
- Class attribute is corrupted for RADIUS accounting messages since ISSU to Junos OS Release 19.1 or later on MX Series platforms. [PR1624066](#)
- RADIUS Change of Authorization (CoA) NAK might not be sent with the configured source address in a virtual-router environment. [PR1625858](#)
- BNG does not correctly issue the statement alarm to APM when condition is met. [PR1626632](#)
- ESSM sessions may get terminated in Radius as class attribute has got corrupted after performing ISSU. [PR1626718](#)
- When connectivity between BNG and APM is lost, the BNG does not regenerate pool drained alarms to APM. [PR1627974](#)

User Interface and Configuration

- A low privileged user can elevate their privileges to the ones of the highest privileged j-web user logged in. [PR1593200](#)
- Junos OS upgrade might fail with error **configuration database size limit exceeded**. [PR1626721](#)

VPNs

- The multicast route is not getting installed after exporting the secondary routes from one instance to another. [PR1562056](#)
- Wrong st0 IFL deletion at spoke when multiple VPNs negotiate same destination address as TS. [PR1601047](#)
- Authentication might fail on bringing up IPsec tunnel when ECDSA is configured in the security ike. [PR1605275](#)
- The rpd process might crash during ISSU if the auto-sensing knob is enabled for l2circuit. [PR1626219](#)

Resolved Issues: 21.3R1

IN THIS SECTION

- [Class of Service \(CoS\) | 113](#)
- [EVPN | 114](#)
- [Forwarding and Sampling | 115](#)
- [General Routing | 115](#)
- [Infrastructure | 127](#)
- [Interfaces and Chassis | 128](#)
- [Intrusion Detection and Prevention \(IDP\) | 129](#)
- [J-Web | 129](#)
- [Juniper Extension Toolkit \(JET\) | 129](#)
- [Junos Fusion Enterprise | 129](#)
- [Layer 2 Ethernet Services | 129](#)
- [MPLS | 129](#)
- [Network Address Translation \(NAT\) | 130](#)
- [Network Management and Monitoring | 130](#)
- [Platform and Infrastructure | 130](#)
- [Routing Policy and Firewall Filters | 131](#)
- [Routing Protocols | 132](#)
- [Services Applications | 134](#)
- [Subscriber Access Management | 134](#)
- [Unified Threat Management \(UTM\) | 135](#)
- [User Interface and Configuration | 135](#)
- [VPNs | 135](#)

Class of Service (CoS)

- Traffic might drop when you activate or deactivate the target-mode using the `set chassis satellite-management fpc [] target-mode` command. [PR1593059](#)
- The child `mgd` processes might become nonresponsive when multiple sessions continuously ask for interface information. [PR1599024](#)

- Traffic loss might occur if you configure the per-unit-scheduler on the aggregated Ethernet interface. [PR1599857](#)
- 802.1p rewrite policies might not have any effect if the rewrite gets tied to circuit cross-connect interfaces. [PR1603909](#)

EVPN

- Prefix added to the output of the `mhevpn.evpn.0` route table triggers TC failure. [PR1566429](#)
- The label field for the EVPN Type 1 route gets set to 1. [PR1594981](#)
- The multicast traffic loss might occur in the EVPN VXLAN scenario with the CRB multicast snooping. [PR1570883](#)
- Configuring the `static-mac` and `no-mac-learning` simultaneously on the VXLAN interface causes stale MAC/IP entry in the EVPN database. [PR1576147](#)
- Sometimes BUM traffic that comes through the EVPN-MPLS tunnel gets dropped or duplicated when the traffic goes out of the aggregated Ethernet interface after the tunnel termination when the aggregated Ethernet interface members span across multiple Packet Forwarding Engines. [PR1578314](#)
- The `rpd` process might crash if the EVPN routing instances or BGP connections flaps. [PR1581674](#)
- Multicast traffic loss might occur in the EVPN setup with IGMP snooping. [PR1582134](#)
- After device reboots in the EVPN VXLAN setup with a graceful restart, the EVPN routes do not get advertised to the EVPN peers until the `rpd` process goes up for 180 seconds. [PR1586246](#)
- The BUM traffic might lose after triggering NSR in the EVPN MPLS or EVPN-ETREE scenario. [PR1586402](#)
- The traffic might be dropped when the EVPN and Layer 3 VPN routes gets resolved using the same MPLS-over-UDP tunnel. [PR1587204](#)
- The traffic might be dropped in the EVPN VXLAN multihomed scenario. [PR1590128](#)
- Traffic loss might occur in the EVPN-VxLAN scenario when the MAC-IP moves from one CE interface to another. [PR1591264](#)
- Transit traffic gets dropped after you disable one of the PE-CE device link on a remote multihome PE device in the EVPN-MPLS A-A setup with Dynamic-List NextHop configured. [PR1594326](#)
- EVPN might not work properly in the multihome setup. [PR1596723](#)

Forwarding and Sampling

- Logical interface statistics for an aggregated sonet displays double value than expected. [PR1521223](#)
- User-defined ARP policer are not applied on the aggregated Ethernet interface until the firewall process restarts. [PR1528403](#)
- The l2ald process might crash when you change the routing-instance. [PR1584737](#)
- The snmpwalk process might not get polled in the mib for some logical child interface. [PR1601761](#)

General Routing

- Routing Engine switchover does not work as expected while SSD fails. [PR1437745](#)
- Memory leaks might be observed on the l2cpd process when you perform certain LLDP operations. [PR1608699](#)
- The auto-sensed L2-BSA subscribers over dynamic-vlan interface might fail after clearing the client on PS ifl for the single-vlan tag. [PR1609844](#)
- The authd process and RADIUS might have stale Layer 2 BSA subscriber entries. [PR1610476](#)
- The DNS-sinkhole functionality does not work since the service PICs are unable to come up when you configure the dnsf package under the chassis configuration. [PR1612316](#)
- After FPC, over subscription of the new subscribers might not be able to connect. [PR1607056](#)
- TCP traffic might be dropped on the source port range 512 to 767 when you configure the flowspec IPv6 filter. [PR1607185](#)
- In the subscriber management scenario, under a rare condition, the Routing Engine reboots and generates a vmcore. [PR1607282](#)
- Jflow-syslog for CGNAT uses 0x0000 in the IPv4 identification field. [PR1602528](#)
- The bbesmgd process generates core file after the Routing Engine goes down. [PR1596848](#)
- On MX10016 router, the SFB Plane not online alarm gets generated after the primary Routing Engine switchovers. [PR1597630](#)
- The following error message might appear periodically in the chassisd logs:

```
CHASSISD_FRU_IPC_WRITE_ERROR: fru_send_msg: FRU GNF 2, errno 40, Message too long
```

[PR1576173](#)

- Fabric link training might occur if the fabric selfping silently gets discarded. [PR1590054](#)
- SSL-FP logging for non SNI session occurs. [PR1442391](#)
- Configuring two IPsec gateways for V1 and V2 triggers IKEv1 client tunnels and AutoVPN hub always checks with IKEV2 policy and not on IKEV1. [PR1465970](#)
- Inaccurate allocated memory for nh and dfw_rulemask under kernel might occurs. [PR1475478](#)
- On MX204 router, incorrect log message for PIC1 appears when you change the configuration from PIC mode to port mode. [PR1500429](#)
- VCCV Type 1 connectivity verification is not supported. [PR1503724](#)
- When you configure the SR-sid ingress sensors, mpls-label does not get reaped out. [PR1516811](#)
- Set of information level Orphan (no password entry) cron logs appears every 1 minute. [PR1527266](#)
- Kernel crash might occur after NSSU when you perform GRES. [PR1533874](#)
- The show chassis alarms command must redirect to the show system alarm command. [PR1536020](#)
- Port mirroring stops working for the fti interface when you change the gre source. [PR1536223](#)
- The sessions creation rate gets set to minimal rate after IDS and CPU throttles in a place during DDoS attack. [PR1544489](#)
- The VM host platform might crash continuously after you upgrade or downgrade, and then boot up with the new image. [PR1544875](#)
- The show system core-dumps command needs to support cRPD. [PR1546097](#)
- The 40G or 100G interfaces might flap during ISSU if you deactivate PTP on the interfaces. [PR1546704](#)
- FPC might crash after the multicast traffic flaps. [PR1548972](#)
- When the MX Series device is in the SAEGW-U mode, in rare cases of a double back-to-back failover involving GRES and Node Association release, some access-peers might not be freed (even after the sessions count associated with that peer reaches zero). [PR1549689](#)
- Deletion or deactivation of the ps interface must not be allowed when the BBE subscriber uses the interface. [PR1550915](#)
- Silent compact flash (/dev/ada1) might fail during reboot or startup of a router. [PR1551171](#)
- The interface might not come up with 1G optics. [PR1554098](#)

- The following error messages occurs on the vty when you commit the CLI commands to fetch host route scale:

```
Cattle-Prod Daemon received unknown trigger (type Semaphore, id 1)
```

[PR1554140](#)

- The device NMI watchdog kicks in after USB scratch installs and wait for the user action to reboot, resulting in a system exception. [PR1555142](#)
- FPC with power related faults might become online again once the Fabric Healing becomes offline. [PR1556558](#)
- On the MPC9E line card, core file is generated when SFB becomes online after ISSU of a GNF. [PR1556627](#)
- The MAC addresses learned in a Virtual Chassis might fail due to aging out in the MAC scaling environment. [PR1558128](#)
- Some transmitting packets might get dropped due to the disable-pfe action being invoked when the fabric self-ping fails. [PR1558899](#)
- The device might run out of service post GRES/ISSU. [PR1558958](#)
- The PIC in the MX-SPC3 line card might get stuck in the Offline status after the flowd process crashes.
- On the MPC10E line cards, interface is unable to send or receive packets after repeated flapping of the 100G link. [PR1560772](#)
- When you abort ztp using the `commit configuration` command, the configuration must persist. [PR1561142](#)
- SPC3 is not supported in Junos OS Release 21.1R1 and Junos OS Release 20.4R2 for deployment. [PR1561188](#)
- The Layer 2 interface information does not get included in the DHCPv4 option-82 circuit-id/remote-id and DHCPv6 relay-agent-interface-id/relay-agent-remote-id options when the service provider style configuration for switch interfaces gets employed. [PR1564010](#)
- Commit error appears when you configure the tunnel-service on a PIC without explicit bandwidth. [PR1565034](#)
- The MX150 device might reboot after you issue the `request system snapshot recovery` command. [PR1565138](#)

- On MX2010 or MX2020 router, the following error message might be observed after switchover with GRES/NSR:

```
CHASSISD_IPC_FLUSH_ERROR
```

[PR1565223](#)

- The `show pfe statistics traffic` command displays incorrect output. [PR1566065](#)
- The license-check process generates core file on the Routing Engine 1 during runtime removal of CB[0] SAM FPGA from the PCIe device. [PR1567066](#)
- The sub line cards (SLC) might reboot after loading the configured inline services and services along with the dfwd filters. [PR1567313](#)
- Drop counts in the `show interfaces voq ae0` command might not match with the `show interfaces queue` command when you issue the `clear interface` command with flowing traffic. [PR1567598](#)
- The MAC addresses might not be relearned successfully after the MAC address age timeouts. [PR1567723](#)
- The chassisd process generates core file with the MPC11 line card moved alternatively from full FPC to SLC mode on GNF. [PR1569206](#)
- The user script output must be logged during the ZTP execution for determining failure in the logs. [PR1570167](#)
- The bbe-smgd process might crash after committing several thousand addresses in a filter term. [PR1570536](#)
- PDB pull or synchronization does not occur in the new primary Routing Engine during unified ISSU. [PR1570841](#)
- Packet loss might occur when you use the sample based action in the firewall filter. [PR1571399](#)
- The BGP sessions might intermittently flap if you enable the egress sFlow sample at a high sampling rate. [PR1571636](#)
- Packets with the MAC address of eth0 and macvlan0@eth0 interface might be sent out to the management interface on the VMHOST platform with NG-RE. [PR1571753](#)
- Router must not boot up with the USB installation again after you select the second option Type reboot and hit return to complete the installation. [PR1571930](#)
- High CPU usage might occur on rpd for routes that uses static subscriber. [PR1572130](#)
- DCI traffic loss of hundred percent occurs in the transit spine devices. [PR1572238](#)

- FPCs restarts automatically after ungraceful removal of SIBs. [PR1572431](#)
- The `show services mobile-edge sessions summary access-network-peers` command displays incorrect established subscriber output after the UPF Handover ENB step. [PR1572520](#)
- A traffic loop might be observed after the VCP interface flaps. [PR1573047](#)
- Some MPC4E-3D line cards displays the following error message at boot up:

```
si5374 clock PLL lock timed out
```

[PR1573729](#)

- Only the root user can execute commands on the host using `vhclient`. [PR1574240](#)
- QSFP 4x10G interface might not come up after FPC reboot. [PR1574279](#)
- DS-Lite throughput degradation might occur on MS-MPC. [PR1574321](#)
- On MX MS-MIC/MPC line cards, the `mpls-template` for jFlow version 9 cannot make a similar template to `mpls-ipv4-template` template. [PR1574402](#)
- PTP might become nonresponsive in the Phase acquiring state after the ISSU upgrade. [PR1575055](#)
- The `rpdp` process might continuously crash if you delete the forwarding-class policy with the discard action. [PR1575177](#)
- When you configure `child inactivity-timeout` under the custom ALG configuration, the configuration does not take effect. [PR1575183](#)
- The MPC10E line cards generates the following error message:

```
user.err aftd-trio: [Error] Em: root: Insert entry failed, entry:parentToken:747441
entryMask:ffffffffffffffff index:52.
```

[PR1575310](#)

- On MX150 router, the interface might take a long time to power down while rebooting, powering-off, halting, or upgrading. [PR1575328](#)
- When you remove an interface and add the interface from the aggregated Ethernet interface bundle, invalid status gets displayed in the output of the `show interface statistics` command. [PR1575623](#)

- The `show services service-sets statistics syslog` command returns the following error message as the service-set does not have the syslog configuration:

```
error: usp_ipc_client_rcv_ 1237: ipc_pipe_read fails! error:No error: 0(0), tries:1.
```

[PR1576044](#)

- IPsec tunnel does not get established when the proxy-id list is received. [PR1576071](#)
- On MX10016 router, when the Fan X Failed alarm gets cleared in the Fan Tray 1, the Fan/Blower OK SNMP alarms gets generated for the Fan Tray 0 [Fan 31 - 41] and Fan Tray 1 [Fan 11 - 41]. [PR1576521](#)
- Mirrored packets gets corrupted when you apply a filter with the port-mirror action and discard. [PR1576914](#)
- The MS-MPC/SPC3 line cards might reset on receiving the subscriber traffic. [PR1576946](#)
- When you apply the imon firewall instance in the egress direction on the family VPLS interface, InputInt gets reported incorrectly. [PR1577212](#)
- Traffic loss might occur when the subscriber service is over the aggregated Ethernet bundle interface(s). [PR1577289](#)
- After optics OIR, some of the channels displays additional link flap. [PR1577676](#)
- Native sensors does not work for ldp lsp, and ldp p2mp sensor. [PR1577931](#)
- The bbe-smgd process might crash when the RADIUS server sends multiple CoA. [PR1578162](#)
- TACACS traffic might get dropped. [PR1578579](#)
- Kernel might become nonresponsive if multiple master Routing Engine switchovers in a short span of time. [PR1578693](#)
- The MPC11E line card might fail to upgrade. [PR1578987](#)
- High FPC CPU usage might occur when signal on the link gets unstable. [PR1579173](#)
- FPC status LED does not turn RED with the power fault. [PR1579466](#)
- The dcpfe process might crash when any interface flaps. [PR1579736](#)
- On the MPC11E line cards, system resource monitor does not list some of the available Packet Forwarding Engines. [PR1579975](#)
- The MPC7E, MPC8E, MPC9E, amd MPC11E line cards might get stuck in the Unresponsive state in a Junos Node Slicing setup. [PR1580168](#)

- The Inline Jflow Routing Engine command gets handled at low priority than the routes and nexthops learning. When the Packet Forwarding Engine gets busy while downloading the routes and nexthops (for example, commit, route convergence and link flap), the inline jFlow related status command or query might get timed out. This error message is harmless and indicate status query did not succeed. [PR1580362](#)
- FPC becomes nonresponsive in the Online state and continuously reboots during ISSU. [PR1580374](#)
- When you map the analyzers to the channelized port, mirror might not work properly. [PR1580473](#)
- More than one subscriber on the same VLAN fails to apply the same FWF template. [PR1580826](#)
- The traffic related to the native VLAN might be dropped. [PR1581075](#)
- Memory leak might occur due to stale NAT64 entries. [PR1581231](#)
- Hitting with vmcore.0 at 0xffffffff80443eef in kern_reboot occurs. [PR1581260](#)
- The timingd process might crash post NSR. [PR1581270](#)
- The rpd process might crash on the new primary Routing Engine after graceful switchover. [PR1581878](#)
- Changing the bandwidth statement does not take affect for the SNMP ifHigSpeed oid until you disable and enable a PSX interface. [PR1582060](#)
- The rpd process might crash when you configure routing-options transport-class. [PR1582081](#)
- The voice VLAN might not get assigned to the access interface. [PR1582115](#)
- Communication between two CE devices might fail when you enable the BGP rib-sharding. [PR1582210](#)
- The rpd process might become nonresponsive due to the race condition. [PR1582226](#)
- The pciephy and firmware download do not work after migration to 6.5.19. [PR1582244](#)
- The bbe-smgd process might crash after the subscriber logs out due to a rare timing issue. [PR1582356](#)
- On MX960 devices, the 400G and 4x100G optics laser restores after reboot despite configuring the disabled interface. [PR1582418](#)
- Traffic might drop with SPC3 in the DS-LITE scenario. [PR1582447](#)
- Destination port might be incorrectly set on the MS-MPC or MS-MIC line cards in the DS-LITE scenario. [PR1582595](#)

- Configuration or removal of the hierarchical-scheduler or per-unit-scheduler might cause traffic to stop forwarding. [PR1582724](#)
- Load balancing does not work correctly on the AMS interfaces for CGNAT traffic On MX USF mode with SPC3. [PR1582764](#)
- The 1x100G, 2x100G, or 3x100G mode might not work when you use the QSFP56-DD 4x100G optics on an interface. [PR1583200](#)
- The next hop of static LSP for MPLS might get stuck in the Dead state after you change the network mask of the outgoing interface. [PR1583245](#)
- On MX150 router, the bcmd process might crash. [PR1583281](#)
- New master Routing Engine might get stuck in the Switchover is in transition and Please wait state after the master reboot test case if the switchover occurs back-to-back within 2 to 3 seconds. [PR1583347](#)
- SNMP SysObjectID.0 gets empty when you enable unified-services. [PR1583534](#)
- The FRR convergence number becomes high with ALB enabled on the aggregated Ethernet interface bundle. [PR1583866](#)
- TCP connection to syslog server might fail to establish after you add the tcp-log configuration for an existing service-set. [PR1583979](#)
- The Layer 2 multicast VXLAN instance goes down since local vtep logical child interface is not associated to the EVPN instance. [PR1584109](#)
- The jsd process consumes full CPU utilization. [PR1584357](#)
- Traffic might not get filtered properly when you configure the security-intelligence profile. [PR1584377](#)
- The rpd process might crash due to a rare timing issue if you enable both the BGP Local-RIB and Adjacency-RIB-In route monitoring in BMP. [PR1584560](#)
- SIB state might not get updated properly when you physically remove the SIB from chassis during SWO. [PR1584706](#)
- Bridge domain names information does not displayed properly in the show bridge statistics instance command. [PR1584874](#)
- After changing the configuration, the show bridge statistics command displays extremely larger value. [PR1584876](#)
- Traffic impact might occur when you configure the tunnel-services bandwidth. [PR1584969](#)

- The vmcore process might generate core file after switchover. [PR1585436](#)
- The secure web proxy continues to send the DNS query for the unresolved DNS entry even after removing the entry. [PR1585542](#)
- GRE OAM packets are sent through queue 0 with the force-control-packets-on-transit-path statement enabled. [PR1586169](#)
- On the MPC2E line cards, traffic drops after enabling the flexible-queuing-mode. [PR1586403](#)
- The following error message appears on certain scenarios when the rpd or GRES restarts with NSR enabled:

```
RPD_KRT_KERNEL_BAD_ROUTE
```

[PR1586466](#)

- The l2ald process might crash when you change the routing-instance. [PR1586516](#)
- Inter and intra VNI traffic might drop in spine with the EVPNVXLAN CRB configuration. [PR1586537](#)
- The rpd process might generate core file if you execute the show igmp continuous stats command after GRES. [PR1587023](#)
- The mspmand.core.ms32.0.gz process might generate core file when you test the memory-usage prints garbage value. [PR1587103](#)
- The SNMP trap for MAC notifications might not be generate when you add an interface explicitly under the switch-options. [PR1587610](#)
- The bbe-smgd process might crash if the staled ACI-based subscribers does not get cleaned up properly. [PR1587792](#)
- The rpd process might crash on the router running a scaled setup. [PR1588439](#)
- The bbe-statsd process might leak memory on the backup Routing Engine during the subscribers login or logout. [PR1589081](#)
- The jsd process might crash in a rare condition in a telemetry scenario. [PR1589103](#)
- The l2cpd process might crash. [PR1589216](#)
- Traffic loss might occur for the interface configured in the subnet 137.63.0.0/16. [PR1590040](#)
- The output of the open configuration BGP route community command displays incorrectly when you use large BGP communities. [PR1590083](#)
- VXLAN DDoS violation might occur when you disable the port mirror analyzer interface. [PR1590150](#)

- Sensor statistics might not be displayed accurately in the `show network-agent statistics operational` command for the data generated from the multiple nodes. [PR1590249](#)
- Even before the FPC or SLC comes online fully during phase 2 of fabric healing and fabric healing, the restart-action gets completed. [PR1590335](#)
- Traffic loss might be observed due to FPC crash in a scaled subscriber scenario. [PR1590374](#)
- Non-zero values might be displayed against the drop field in the `show network-agent statistics` command post switchover scenarios. [PR1590432](#)
- NAT service might not occur after AMS switchover or deactivating/activating NAT service. [PR1590890](#)
- The orchagent and syncd processes might crash when you delete the routes. [PR1590983](#)
- Traffic loss might occur post the SAK keys change. [PR1591432](#)
- If you configure the COS CR-features used by VBF service, MPC might crash with the subscriber. [PR1591533](#)
- Frequent phydriver sync_state toggling results in high two way time errors. [PR1591667](#)
- The `clear-ipsec-sas-for-duplicate-ts` command does not clear the Secure Access (SA) for duplicate traffic-selectors (TS). [PR1591735](#)
- FPC goes offline after switchover in the power budget test case. [PR1592004](#)
- The picd log floods when there is Optics does not support configured speed system alarm. [PR1592165](#)
- xSTP might not get configured when enabled on a interface with SP style configuration. [PR1592264](#)
- The aftmand process might crash when you configure an interface with analyzer. [PR1592267](#)
- ZTP occasionally fails to apply user configuration after the system upgrade. [PR1592281](#)
- The mobiled daemon might crash after switchover for an AMS interface or crashes on the service PIC with the AMS member interfaces. [PR1592345](#)
- The Routing Engine kernel might crash due to logical child interface of an aggregated interface adding failure in the Junos kernel. [PR1592456](#)
- The l2cpd agent might become unresponsive after starting the telemetry service. [PR1592473](#)
- Purge timer starts after the prpd client disconnects with the purge timeout set to never. [PR1592591](#)
- Using the BITS interface from the backup Routing Engine for clock recovery might not work. [PR1592657](#)

- The packet coming from the PS interface and forwarding to the SPC3 might be dropped. [PR1592706](#)
- Any mmcq process-based services might crash due to shared memory queues issue in a rare condition. [PR1592889](#)
- Port related component sensor does not get exported when subscribed to the `/components/component/state/path`. [PR1593031](#)
- Low priority host bound traffic might starve or delay processing of high priority host bond traffic. [PR1593083](#)
- The TCP connections to the telemetry server might become nonresponsive in the `Close wait` state. [PR1593113](#)
- The TCP keepalive might not be processed by the private network host. [PR1593226](#)
- IPv6 neighbor might remain unreachable in VRRP for the IPv6 scenario. [PR1593539](#)
- Jweb Deny log nested-application displays unknown instead of the specific application. [PR1593560](#)
- Fabric errors do not get generated after swapping the MPC10E line card with the MPC7E line card in the same slot. [PR1593821](#)
- Packet drop might occur when traffic moves from one FPC to another FPC. [PR1594244](#)
- On MX5, MX40, and MX80 line cards, TEB becomes nonresponsive in the `Present` state. [PR1595107](#)
- Default wavelength for 400G ZR modules displays incorrect value. [PR1595498](#)
- The interface might be delayed after you issue the `set interface interfacename disable` command. [PR1595682](#)
- Firmware might fail to be downloaded to MIC on the MX Virtual Chassis setup. [PR1595693](#)
- The applications might crash if the publishing parent objects linked child objects gets published by the different applications. [PR1595846](#)
- Mismatch in the master and backup Routing Engines with `inetcolour` tables and BGP-SRTE tunnels occurs. [PR1596095](#)
- Packet Forwarding Engine wedge might occur if many IPv4 packets are received that need to be fragmented. [PR1596100](#)
- The `l2ald` process might crash on all the leaves and spines after you add a new leaf to the EVPN fabric. [PR1596229](#)
- The `nsd` process generates core file when you verify the session-limit rate and issue the `bypass-traffic-on-exceeding-flow-limits` command. [PR1596578](#)

- Traffic loss might occur periodically in the MACsec-used setup if the Routing Engine works under a pressure situation. [PR1596755](#)
- The SR-TE tunnel initiated from a non-juniper PCE might fail. [PR1596821](#)
- Traffic fails to recover after multiple quick dot1xd restarts when you enable the MACsec suspend-for option. [PR1596854](#)
- CGNAT MX SPC3 AMS warm-standby 1:1 redundancy problem with CLI CPU statistics lost data after PIC failover occurs. [PR1596976](#)
- The IFD creation fails after you add or delete the invalid speed configuration. [PR1597022](#)
- Major alarms on all FPCs in chassis might appear after some time from the bootup. [PR1597066](#)
- The MAC/IP withdraw route might be suppressed by rpd in the EVPN VXLAN scenario. [PR1597391](#)
- ALG traffic might be dropped. [PR1598017](#)
- Subscriber management daemons might continuously generate core files and shutdown with the invalid Routing Engine sensors configured. [PR1598351](#)
- The afeb process might crash with MIC-3D-8DS3-E3. [PR1598411](#)
- Upper backplane type for the MX2020 router are incorrectly reported as Chassis. [PR1598594](#)
- The packet loop might occur after you receive the PCP request packets, which are destined to software concentrator address. [PR1598720](#)
- Component sensor does not export logs. [PR1598816](#)
- The MX SPC3 applications for protocol ICMP does not get detected and does not allow user to modify inactivity-timeout values. [PR1599603](#)
- The configuration check would fail if you configure more than 8 FCs and enable CBF. [PR1600544](#)
- The multiservices card does not drop the TCP acknowledgment packet received as a reply to the self-generated TCP keepalive. [PR1600619](#)
- Duplicate Address Detection(DAD) flags appears for the IRB interfaces after removing the configuration and restoration, which may lead to traffic blockage. [PR1601065](#)
- The BBE-SMGD process generates core files at bbe_dequeue_and_deliver bbe_process_work_queues bbe_smd_main_post_dispatch. [PR1601203](#)
- Unable to commit configuration due to the Check-out failed error message for the mobility process. [PR1601785](#)
- Few line cards might not come up online with the increased-bandwidth mode. [PR1602080](#)

- The Packet Forwarding Engine might get disabled by a detected major CMERROR event when you ungracefully remove the MIC from MPC2E-3D-NG/MPC3E--3D-NG. [PR1602939](#)
- On MX150 router, interface hold-time up does not work. [PR1604554](#)
- The MPLS transit router might push an extra entropy label to the LSP. [PR1605865](#)
- IRB IFL do not get created after a sequence of events. [PR1565842](#)
- The rpd process might generate core file after the Routing Engine switchovers. [PR1582095](#)
- NSSU performed with MACsec configuration might result in the fxpc process to generate the core file. [PR1603602](#)
- After performing NSSU, the following error message appears when you check the version details:

```
timeout waiting for response from fpc0
```

[PR1584457](#)

- The MVPN traffic loss might occur due to missing of the flooded multicast next-hop. [PR1587054](#)
- The rpdagent process crashes on the primary Routing Engine after enabling multiple GRES with GR/NSR. [PR1593104](#)
- Node name should not be attached to the system hostname under LLDP. [PR1593991](#)
- On MX480 routr, the subinfo process generates core file with the Layer 2 Node Scaling. [PR1598187](#)

Infrastructure

- While loading the kernel, the kernel displays the following error message:

```
GEOM: mmcsd0s.enh: corrupt or invalid GPT detected.
```

[PR1549754](#)

- The fxpc process might crash and generate core [PR1611480](#)
- The Virtual Machine might crash if you share a file between the host operating system and guest operating system using virtFS. [PR1551193](#)
- The vme/me0 management interface cannot process any incoming packets. [PR1552952](#)

Interfaces and Chassis

- On the MPC10 line cards, DMRs or SLRs are not received with an EVPN up MEP on the aggregated Ethernet interface with normalization. [PR1543641](#)
- Configuration check-out fails with the following error message:

```
identical local address found on rt_inst [default], intf
```

[PR1581877](#)

- Traffic might be interrupted while adding the xe or ge interfaces as member of the aggregated Ethernet interface bundle. [PR1569399](#)
- if-media-type is missed from the interface XML output. [PR1574035](#)
- The ARP resolution failure might occur during the VRRP failover. [PR1578126](#)
- The alarm data type of the JVISION optics sensor gets changed from bool_val to str_val. [PR1580113](#)
- Newly added MC-LAGs do not come up after the Routing Engine switchovers. [PR1583547](#)
- When changing the address of the Micro BFD session from IPv4 to IPv6, the BFD session and the aggregated Ethernet interfaces goes down. [PR1584853](#)
- On MX10003 router in the Virtual Chassis mode, you cannot configure the pseudowire interface. [PR1587499](#)
- The dcd process might crash after the Routing Engine switchovers, reboots, or change the management interface configuration. [PR1587552](#)
- The VRRP host cannot be reached if you configure native-vlan-id. [PR1595896](#)
- Duplicate src + dest pair check gets completed only after across the same tunnel encapsulation type for FTI. [PR1599266](#)
- The dcd process might crash and FPC might be stuck in the Ready state. [PR1601566](#)
- The aggregated Ethernet interface might flap when you change the configuration. [PR1602656](#)
- Memory leak on the dcd process occurs when you commit configuration changes on any interfaces in a setup with AMS interface configured. [PR1608281](#)

Intrusion Detection and Prevention (IDP)

- Addition of signature in the packet drop occurs and sends the signature to the record packet drops module. [PR1574603](#)

J-Web

- J-Web allows a locally authenticated attacker to escalate their privileges to root. [PR1511853](#)

Juniper Extension Toolkit (JET)

- GRPC connections gets stuck in the Established state with no active collector. [PR1592542](#)

Junos Fusion Enterprise

- Reverting mastership from the Routing Engine 1 to Routing Engine 0 might crash the l2ald daemon and cause an outage. [PR1601817](#)

Layer 2 Ethernet Services

- The DHCP client becomes offline for 120 seconds after sending the DHCPINFORM message in the DHCP relay scenario. [PR1575740](#)
- DHCP relay drops packets during the renewal DHCP process. [PR1576417](#)
- The jdhcpd process might crash if you enable relay-source 100 in the DHCP relay. [PR1580724](#)
- The traffic received on a port in the LACP detached state might be incorrectly forwarded. [PR1582459](#)
- An ALQ synchronization issue on the primary and backup BNG occurs with the loss of subscriber session redundancy through the ps interface. [PR1583310](#)
- The DHCP ALQ queue might become nonresponsive causing the subscriber to flap. [PR1590421](#)
- The jdhcpd process might not respond to any discover message when the process is in the Clients waiting to be restored state. [PR1592552](#)

MPLS

- The rpd process might crash in the co-routed bidirectional RSVP LSP scenario. [PR1544890](#)
- LDP P2MP traffic might be interrupted post GRES. [PR1609559](#)

- Traffic loss might occur when the rpd process crashes with RVP-signaled P2MP LSP configured. [PR1559022](#)
- The LSP might fail to be established when you enable the ISIS-TE or OSPF-TE. [PR1575060](#)
- Sub-optimal routing issues might occur in case of LDP route with multiple next-hops. [PR1582037](#)
- Need to add support the lsp-ping-multiplier option for LDP-OAM similar to RSVP-OAM. [PR1582254](#)
- MBB do not get triggered when LSP reverts to the primary path. [PR1587704](#)
- The rpd process generates core file in the backup Routing Engine at mirror_process_recvd_data_queue with the mldp NSR configuration. [PR1594405](#)
- The LDP replication session might not get synchronized when you enable the dual-transport. [PR1598174](#)
- Static LDP P2MP might fail after the NSR switchovers. [PR1598344](#)
- The VPLS connection might go down if you configure the dual-transport statement. [PR1601854](#)
- RSVP detour LSP might fail to come up when an LSR in the detour path goes down. [PR1603613](#)
- The rpd process might crash on the standby_re LDP module when you enable the VPLS mac-flush on the peer by default or configuration. [PR1610638](#)

Network Address Translation (NAT)

- Services NAT mappings and sessions are incorrect while checking the SIP sessions from public to private and RTP from private to public. [PR1577922](#)

Network Management and Monitoring

- SNMP reflects outdated ARP entries. [PR1606600](#)

Platform and Infrastructure

- The CoS queue egress interface forwarding-class might not work as expected. [PR1538286](#)
- The PPP/L2TP clients on si-0/4/0 and si-0/5/0 might get disconnected due to keep alive failure. [PR1570053](#)
- The following error message might occur when you configure the adaptive load-balancing on a LAG:

```
HEAP malloc(0) detected!
```

PR1547240

- Upon receipt of specific sequences of genuine packets destined to the device, the kernel crashes and restarts. [PR1557881](#)
- The l2tp tunnel might not work with the filter-based encapsulation. [PR1568324](#)
- The toe_lu_stats_ucode process generates core file at jbeta_fcv_alloc_fcv_idx_global jbeta_sfilter_fcv_cb bwy_dfw_sfilter_fcv_cb. [PR1569328](#)
- FPCs might crash randomly when you delete the interface-set in the system. [PR1571192](#)
- Memory partitioning issue might occur on the Packet Forwarding Engine after applying sampling and flex-flow-sizing to the line cards. [PR1575994](#)
- When you commit source-address addr routing-instance and then delete source-address addr in the private edit mode, the commit fails with a warning message. [PR1582529](#)
- VRRP device as the slave role might cause the destination IP to become unreachable after the VRRP mastership switchovers. [PR1584115](#)
- FPC might crash in a scaled firewall configuration. [PR1586817](#)
- The traffic might not failover when you enable shared-bandwidth-policer on the aggregated Ethernet interface. [PR1588708](#)
- The audit process generates core file when you change the TACACs and login user passwords. [PR1589953](#)
- VLAN tagged traffic might be dropped with the service provider style configuration. [PR1598251](#)
- The service filter might get incorrectly programmed in the Packet Forwarding Engine due to a rare timing issue in the enhanced subscriber management environment. [PR1598830](#)
- The kernel might generate core file if you restart the BGP connections after you delete the BGP authentication. [PR1601492](#)
- Multicast traffic gets dropped when forwarded over VPLS through IRB. [PR1607311](#)

Routing Policy and Firewall Filters

- If you configure the customer-defined routing instance under the name-server, you cannot resolve the DSN name. [PR1539980](#)
- Traffic loss might occur due to rpd crash when the NSR switchovers. [PR1579830](#)
- The bbe-smgd - dynamic-profile NACK due to configuration error might occur when you read the address mask prefix-length in the policy options or policy statement. [PR1583535](#)

- BGP route preference using PBR do not get applied to all the routes when you enable the CCNH Inet6. [PR1596436](#)
- IPv6 firewall filter displays commit error when you configure TC in the binary or hexadecimal format. [PR1597422](#)

Routing Protocols

- BGP session might go down due to BGP-LS TLV received going out of order. [PR1546416](#)
- Multicast traffic might get duplicated on the subscriber interface. [PR1607493](#)
- Some routes might get incorrectly programmed in the forwarding table in the kernel with next-hop installed as DEAD. [PR1601163](#)
- The BGP session terminates upon the receipt of the specific BGP FlowSpec advertisement. [PR1323474](#)
- Incorrect active, received, accepted counters might occur in the output of the show bgp summary. [PR1558678](#)
- The rpd memory leak might occur during the ephemeral commits in the OSPFv2 scenario. [PR1568157](#)
- Incorrect authentication-algorithm set in bgp neighbor [PR1571705](#)
- After the first parallel ISSU, subsequent ISSU aborts with the Aborting Daemon Prepare message. [PR1572265](#)
- The BFD session of DHCP subscriber does not come up on the MPC2E card and remains in the Down state. [PR1572577](#)
- Need to provide a cli option to change the default BGP listen port. [PR1576728](#)
- The unexpected CSPF link becomes down or deletes events on LSPs. [PR1576818](#)
- The rpd might crash when two or more routing instances gets deleted in one shot. [PR1578740](#)
- Short multicast packets drops using PIM when multicast traffic is received at a non-RPT/SPT interface. [PR1579452](#)
- BGP session carrying VPNv4 prefix with IPv6 next-hop might be dropped. [PR1580578](#)
- BGP replication might become nonresponsive in rare and timing conditions. [PR1581578](#)
- The rpd might crash in the BGP and MPLS scenario. [PR1581794](#)
- Traffic might misroute or get dropped after the Packet Forwarding Engine restarts or when the interface flaps. [PR1581845](#)

- CPU utilization might be increased to hundred percentage if more than 10M BGP prefixes are received. [PR1582411](#)
- With IGMP snooping implemented, unexpected jitter issue that could cause traffic loss occurs. [PR1583207](#)
- The SSH cipher option Triple-DES gets disabled in the FIPS mode. [PR1583470](#)
- The rpd process might crash in certain IS-IS scenario. [PR1583484](#)
- On rare occasion, the rpd process might generate core file on the backup Routing Engine after loading a new image. [PR1583630](#)
- Even though when you do not configure the `show task replication` command, the output of the command displays the Origin-validation (RV) replication status. [PR1583692](#)
- The rpd process might crash in the BGP multipath scenario if the single hop EBGP peer goes down. [PR1585265](#)
- The rpd process might crash when you configure the BGP RPKI session record-lifetime less than the hold-time. [PR1585321](#)
- Traffic drop might occur when you configure IS-IS. [PR1585471](#)
- The rpd process might crash after you commit the configured static group 224.0.0.0. [PR1586631](#)
- Incorrect BGP next-hop advertisement occurs in the Layer 3 VPN scenario. [PR1587879](#)
- The multicast traffic loss might occur after ISSU. [PR1588555](#)
- The rpd might crash in BGP multipath scenario if interface for a single hop EBGP peer goes down. [PR1589141](#)
- The rpd might crash in the scaled routing instances scenario. [PR1590638](#)
- The rpd process might crash post GRES. [PR1590912](#)
- PIM joins might not be synchronized between the primary and backup Routing Engines due to the restart of the `ppmd` process. [PR1591685](#)
- Disabling or enabling BGP in a short time interval on a scaled NSR router can result in the backup RPD to restart. [PR1591717](#)
- The rpd process might crash if the BGP peer flaps. [PR1592123](#)
- The remote LFA (loop-free-alternate) backup path might not be formed. [PR1592424](#)
- The routing process might crash due to memory corruption while processing the BGP multipath route. [PR1594626](#)

- The IPv4 static route might still forward traffic unexpectedly even after you delete the static route configuration. [PR1599084](#)
- The rpd process might be stuck at hundred percentage in the OSPFv3 scenario. [PR1601187](#)
- Packet might get drop after changing MTU on the aggregated Ethernet interface. [PR1605376](#)
- With rib-sharding enabled, when you perform any commit, all BGP sessions with 4 byte peer-as flaps (as number 65536 or greater). [PR1607777](#)

Services Applications

- Need to support to clear the l2tp session based on the routing-instance name filter. [PR1580984](#)
- IWF AVP value might not be reflected properly on LTS. [PR1581096](#)
- On MX480 router, the vmcore process generates core file due to doadump (textdump=1) at / volume/build/junos/occam/llvm-5.0/sandbox-204ab-20210401/freebsd/stable_11-204ab/ 20210401.22. [PR1595088](#)
- The **show services l2tp tunnel extensive**, **show services l2tp session extensive** and **show subscribers accounting-statistics** commands do not work on LTS. [PR1596972](#)
- The kmd.core process generates core file at **kmd_gen_fill_sa_pair_sadb_flags @kmd_update_sa_in_kernel @kmd_sa_cfg_children_sa_free**. [PR1600750](#)
- The **show services l2tp tunnel extensive** and **show services l2tp session extensive** commands provide incorrect outputs on LTS. [PR1601886](#)

Subscriber Access Management

- BBE-SMGD configures in-correct vbf_accurate_accounting_bits to the Packet Forwarding Engine. [PR1515899](#)
- Prefix duplication errors might occur for DHCPv6 over the PPPoE subscribers. [PR1609403](#)
- DHCP session fails when you issue the session-limit-per-username statement. [PR1612196](#)
- Subscribers might remain in the **Terminated** state when the RADIUS server becomes unreachable. [PR1600655](#)
- The **Service session entry creation failed** error message appears during ephemeral commit. [PR1603030](#)

Unified Threat Management (UTM)

- No counter available for the `juniper-local default` action. [PR1570500](#)

User Interface and Configuration

- During rare circumstances, the `mgd` process might crash and generate a core file on Junos devices connected with the Contrail Service Orchestration (CSO). [PR1569903](#)
- The `juniper.conf.gz` file gets created with empty data when you create the tenant system. [PR1584850](#)
- Fix fast-diff to detect the change when a deactivated delta-list element gets deleted. [PR1586229](#)
- File copy using FTP does not prompt for password like FreeBSD Junos equivalent. [PR1587646](#)
- The `apply-path` does not expand for the configuration under groups. [PR1592032](#)
- The `mgd` process might crash after you commit check. [PR1593192](#)
- Invalid JSON and XML output formats for the command like `show system resource-monitor ifd-cos-queue-mapping fpc x | display [json|xml]` appears. [PR1605897](#)

VPNs

- Traffic from the reverse direction might cause traffic loss for up to 1 second with NSR switchover. [PR1558395](#)
- The `iked` process might crash when IKEv2 negotiation fails. [PR1577484](#)
- The `rpdpd` might crash in the NG-MVPN scenario. [PR1579963](#)
- The traffic of the Draft-Rosen Multicast VPN might get lost after Routing Engines switchover. [PR1584720](#)
- Unable to add the BGP standard community to NGMVPN Type-6 and Type-7 routes in the VRF export policy. [PR1589057](#)
- The DDoS protection reason packets failed the multicast RPF check might appear in the NG-MVPN scenario with GRE transport. [PR1591228](#)
- The `rpdpd` process might crash if the interface goes down in the BGP-MVPN scenario. [PR1597387](#)
- Authentication fails on bringing up the IPsec tunnel between the DUT and Strongswan-peer with IKE (group21 sha-512 aes-192-cbc) proposal. [PR1605275](#)

Documentation Updates

There are no errata or changes in Junos OS Release 21.3R2 documentation for MX Series routers.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading to Release 21.3R2 | 137](#)
- [Procedure to Upgrade to FreeBSD 12.x-Based Junos OS | 137](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 140](#)
- [Upgrading a Router with Redundant Routing Engines | 140](#)
- [Downgrading from Release 21.3R2 | 141](#)

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 21.3R2

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-
x86-32-21.3R2.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-
x86-64-21.3R2.9-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-
x86-32-21.3R2.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-
x86-64-21.3R2.9-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 21.3R2, 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 21.3R2 `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

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

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 21.3R2

To downgrade from Release 21.3R2 to another supported release, follow the procedure for upgrading, but replace the 21.3R2 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the [Installation and Upgrade Guide](#).

Junos OS Release Notes for NFX Series

IN THIS SECTION

- [What's New | 142](#)
- [What's Changed | 143](#)
- [Known Limitations | 143](#)
- [Open Issues | 144](#)
- [Resolved Issues | 145](#)
- [Documentation Updates | 147](#)
- [Migration, Upgrade, and Downgrade Instructions | 147](#)

These release notes accompany Junos OS Release 21.3R2 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

IN THIS SECTION

- [What's New in 21.3R2 | 142](#)
- [What's New in 21.3R1 | 142](#)

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

What's New in 21.3R2

There are no new features or enhancements to existing features for NFX Series devices in Junos OS Release 21.3R2.

What's New in 21.3R1

IN THIS SECTION

- [Application Identification \(AppID\) | 142](#)

Application Identification (AppID)

- **First-packet classification in advanced policy-based routing (APBR) (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.3R1, APBR uses first-packet classification to identify applications in network traffic. APBR identifies applications by examining the very first packet in the traffic flow and then applies application-specific rules to forward the traffic.

With first-packet classification, you can steer the traffic accurately and efficiently over the network, optimizing network link utilization and boosting the performance.

See [[Advanced Policy-Based Routing Overview](#).]

- **IPv6 address support in application quality of experience (AppQoE) (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.3R1, you can use IPv6 addresses in AppQoE configurations. The support includes:

- IPv6 address in overlay path configuration
- Active probing sessions using IPv6 addresses as source and destination address.
- IPv4 and IPv6 traffic from the client side
- Dual stacking of IPv4 and IPv6 on the LAN side
- IPv6 address on the LAN side for SaaS (software as a service) probing

See [[Application Quality of Experience.](#)]

- **IPv6 traffic for application-based multipath routing (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.3R1, we support application-based multipath routing in the following IPv6 use cases:
 - IPv6 traffic over IPv6 tunnels
 - Application-based multipath routing over direct IPsec tunnels without GRE for IPv6 traffic
 - Application-based multipath routing over direct GRE tunnels without IPsec for IPv6 traffic
 - Application-based multipath routing over MPLS-over-GRE-over-IPsec for IPv6 traffic

See [[Application-Based Multipath Routing.](#)]

What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.3R1 and 21.3R2 for NFX Series devices.

Known Limitations

There are no known limitations in hardware and software in Junos OS Release 21.3R1 and 21.3R2 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

- [General Routing](#) | 144
- [High Availability](#) | 144

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

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

General Routing

- On the NFX350, if you change the device operational mode to custom mode, ovs-vswitchd cores might be seen on the device. [PR1634245](#)
- At times, L3 interfaces on the NFX150 device do not receive traffic when the SRIOV mapping changes from L2 interface to L3 interface. [PR1612643](#)

High Availability

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

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 145](#)
- [Resolved Issues: 21.3R1 | 145](#)

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

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

Resolved Issues: 21.3R2

IN THIS SECTION

- [Interfaces | 145](#)

Interfaces

- L3 dataplane interfaces are not appearing when flex mode is enabled on NFX350-S3 devices. [PR1599643](#)
- The data displayed by the CLI command `show system visibility jcp` in the JCP Interfaces, JCP Interfaces Statistics, and JCP Disk Information sections is shifted to the right by one column. [PR1600414](#)

Resolved Issues: 21.3R1

IN THIS SECTION

- [General Routing | 146](#)
- [Interfaces | 146](#)
- [Performance Modes | 146](#)

General Routing

- RPD core file is generated when the device reboots and daemon restarts. Daemon recovers and there is no service impact on routing protocol usage. [PR1567043](#)
- IPsec tunnel is not established when receiving the proxy-id list. [PR1576071](#)

Interfaces

- AE interface statistics are not reported on NFX250 devices. [PR1581596](#)
- LACP subsystem is not enabled in NFX250 NextGen devices. [PR1581717](#)
- On NFX Series devices, you need to adjust MTU sizes of the OVS system interfaces to maintain consistency. [PR1586967](#)
- Unable to configure destination-port on firewall filter on NFX250 NextGen devices. [PR1592019](#)
- On NFX Series devices, deletion of VNF interfaces that are mapped SR-IOV interface fails. [PR1598993](#)
- L3 dataplane interfaces are not appearing when flex mode is enabled on NFX350-S3 devices. [PR1599643](#)

Performance Modes

- You cannot enable the trust mode on an SR-IOV virtual function assigned to a VNF. [PR1593037](#)

Virtual Network Functions (VNFs)

- On NFX Series devices, while configuring `vmhost vlans` using `vlan-id-list`, the system allows duplicate VLAN IDs in the VLAN ID list. [PR1438907](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R1 and 21.3R2 documentation for NFX Series documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 147](#)
- [Basic Procedure for Upgrading to Release 21.3 | 148](#)

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

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

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 21.3

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 21.3R2:

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

- [What's New | 149](#)
- [What's Changed | 153](#)
- [Known Limitations | 159](#)
- [Open Issues | 160](#)
- [Resolved Issues | 162](#)
- [Documentation Updates | 168](#)
- [Migration, Upgrade, and Downgrade Instructions | 168](#)

These release notes accompany Junos OS Release 21.3R2 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

- [What's New in 21.3R2 | 150](#)
- [What's New in 21.3R1 | 150](#)

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

What's New in 21.3R2

There are no new features or enhancements to existing features in Junos OS Releases 21.3R2 for PTX Series routers.

What's New in 21.3R1

IN THIS SECTION

- [IP Tunneling | 150](#)
- [Junos Telemetry Interface | 150](#)
- [MPLS | 151](#)
- [Routing Policy and Firewall Filters | 151](#)
- [Routing Protocols | 151](#)
- [Source Packet Routing in Networking \(SPRING\) or Segment Routing | 152](#)
- [Services Applications | 152](#)
- [Additional Features | 153](#)

IP Tunneling

- **Support for IP-over-IP tunnel stitching (MX Series, MX240, MX480, MX960, PTX1000, PTX10008, PTX10016, and QFX10002)**—In Junos OS Release 21.3R1, we introduce IP-over-IP tunnel stitching. You can use this feature to terminate an IP-over-IP tunnel on a device and initiate another tunnel on the same device. When a device receives the IP-over-IP packet, it de-encapsulates the outer packet header and inner packet lookup occurs. The inner IP packet header then points to another tunnel on the same device, where the same device encapsulates the packet again with another IP-over-IP header.

[See [Overview of Next-Hop-Based Dynamic Tunneling Using IP-Over-IP Encapsulation](#).]

Junos Telemetry Interface

- **Telemetry stream path resolution by MPLS and RSVP interfaces (ACX710, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5448, ACX4558-D, ACX5448-M, MX150, MX204, MX340, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, vMX, PTX1000, PTX3000, PTX5000, PTX10002-60C, and PTX10008)**—Starting in Junos OS Release 21.3R1, you can

choose to stream telemetry statistics only for MPLS and RSVP-enabled interfaces. Use the resource path `/network-instances/network-instance/mpls/signaling-protocols/rsvp-te/interface-attributes/interface/admin-status`.

[See [Configuring a Junos Telemetry Interface Sensor \(CLI Procedure\)](#) and [Telemetry Sensor Explorer](#).]

MPLS

- **RSVP updates available bandwidth values without notifying IS-IS (MX960, MX2010, MX2020, PTX1000, PTX10001, PTX10008, and PTX10016)**—When RSVP label-switched paths (LSPs) and segment routing LSPs coexist on a link, RSVP takes into account how much bandwidth the segment routing LSPs use. By default, RSVP updates the values for the local unreserved bandwidth and the maximum available bandwidth and passes the values on to IS-IS. Starting in Junos OS Release 21.3R1, you can configure RSVP to update available bandwidth values without notifying IS-IS if the bandwidth change is within a certain threshold configured at the `[edit protocols rsvp interface interface-name update-threshold-max-reservable]`.

If you configure the `local-bw-override-threshold` statement at the `[edit protocols rsvp interface interface-name non-rsvp-bandwidth]` hierarchy level, RSVP always updates the available bandwidth values. However, it reports only the new values to IS-IS if the bandwidth change passes the threshold.

[See [update-threshold-max-reservable](#) and [local-bw-override-threshold](#).]

Routing Policy and Firewall Filters

- **Support for discard interfaces (QFX-Series and PTX-Series)**—Starting in Junos OS Release 21.3R1, you can configure a discard interface for IPv4 and IPv6 traffic, which you can then use in a local policy for handling unwanted packets.

[See [Configuring Discard Interfaces](#).]

Routing Protocols

- **Check for AS match in BGP policy AS paths without using regular expressions (ACX5048, ACX5096, ACX5448, MX240, MX480, MX960, MX2008, MX10016, vMX, PTX1000, PTX5000, PTX10001, PTX10002, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, and QFX10016)**—Starting in Junos OS Release 21.3R1, you can configure BGP policies to check for an autonomous system (AS) match in an AS path without using regular expressions. The BGP policy compares the AS to an AS-list or AS-list-group and returns true if it finds a match. You can configure the BGP policy to check for a matching origin, neighbor, or transit AS. This feature provides a faster alternative to match origin, transit, and peer AS numbers than using a regular expression.

Configure this feature using the `as-path-neighbors`, `as-path-origins`, or `as-path-transits` option at the `[edit policy-options policy-statement policy-name from]` hierarchy level. For each type of match, use `(as-list |`

`as-list-group`) `as-list-name/as-list-group-name` to specify the list or group of AS paths to compare the match to. Configure the AS list or AS group at the `[edit policy-options]` hierarchy level.

[See [policy-options](#) and [policy-statement](#).]

- **Maximum reference bandwidth increased to 4 TB for IGP protocols (ACX710, ACX5448, MX960, MX2020, MX10003, PTX5000, and PTX1000)**—Starting in Junos OS Release 21.3R1, we've increased the maximum reference bandwidth for IS-IS and OSPF IGP protocols from 1 Tbps to 4 Tbps. The default bandwidth is 100 Mbps. You can increase the reference bandwidth to adjust the path metrics, which you use to determine the preferred path in case of multiple equal-cost routes to a destination.

To configure the reference bandwidth, use the `reference-bandwidth` *reference-bandwidth* statement at the `[edit protocols isis]` hierarchy level or the `[edit protocols (ospf | ospf3)]` hierarchy level.

[See [reference-bandwidth \(Protocols IS-IS\)](#) and [reference-bandwidth \(Protocols OSPF\)](#).]

- **Support for route target (RT) multipath (MX Series and PTX Series)**—Starting in Junos OS Release 21.3R1, the BGP RIB sharding supports route target (RT) multipath and dependent features such as protect-core and policy-based multipath. RT multipath does load balancing by combining next hops from multiple component routes to form a forwarding-only route. When you enable sharding, both the shard and the main threads participates in this process of creating the forwarding-only route.
- **BMP with BGP Sharding and Update IO (JRR Series, MX Series, PTX Series, and vMX)**— Starting in Junos OS Release 21.3R1, we support AdjOutRIBs (pre and post policy tables) through BGP Monitoring Protocol (BMP).

[See [BGP Monitoring Protocol](#).]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Support for Application Specific Link Attributes (ASLA) for flexible algorithms (ACX710, MX204, MX240, MX480, MX960, MX10003, MX 10008, MX10016, MX2008, MX2010, MX2020, PTX1000, PTX5000, PTX10002, PTX10008, PTX10016, VMX)**: IS-IS supports advertising different te-metric and admin-groups for RSVP and flexible algorithm on the same link using flexible-algorithm specific ASLA as defined in RFC 8919.

[See [strict-asla-based-flex-algorithm](#) <https://www.juniper.net/documentation/us/en/software/junos/is-is/topics/ref/statement/protocols-isis-source-packet-routing-strict-asla-based-flex-algorithm.html>.]

Services Applications

- **Changes to inline active flow monitoring (PTX Series)**—Starting in Junos OS Release 21.3R1, by default no flows are maintained, thereby increasing the number of packets that can be processed.

Every sampled packet is considered to be a flow. When the sampled packet is received, the flow is created and immediately timed out as inactive, and the software exports a record to the collector. Therefore, the number of records sent to the collector is higher than before. The IPFIX and version 9 Options Template Data Record now contains 0 in the Flow Active Timeout (36) and Flow Inactive Timeout (37) fields. Therefore, the Options Template Data Record is not compliant with IPFIX RFC 7011.

The `show services accounting flow inline-jflow fpc-slot slot-number operational mode` command now displays 0 for all of the Active Flows and Timed Out fields. The values of the various Total Flows fields are now equal to their respective Flow Packets field values. The values of the various Flows Inactive Timed Out fields are now equal to their respective Flow Packets field values.

To change this default behavior and once again create and maintain flows, configure the `nexthop-learning` statement at the `[edit services flow-monitoring version- version template template-name]` hierarchy level. Then attach that template to all sampling instances associated with FPCs that require the previous behavior.

[See [Understanding Inline Active Flow Monitoring](#).]

Additional Features

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

- **MSDP support** (PTX10001-36MR, PTX10004, and PTX10008)
 - Nonstop Active Routing (NSR) with MD5 authentication
 - MSDP peer authentication
- **TWAMP Light IPv6 addressing support** (ACX710, ACX2000, ACX2100, ACX5448, MX5, MX10, MX40, MX80, MX104, MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10008, MX10016, vMX, PTX1000, and PTX5000)

[See [Understanding MSDP](#).]

[See [Understand Two-Way Active Measurement Protocol on Routers](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.3R2](#) | 154

- [What's Changed in Release 21.3R1 | 155](#)

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

What's Changed in Release 21.3R2

IN THIS SECTION

- [General Routing | 154](#)
- [Network Management and Monitoring | 154](#)
- [User Interface and Configuration | 155](#)

General Routing

- **New Commit check for Layer 2 Interfaces (PTX10003)**— We've introduced a commit check to prevent you from misconfiguring ethernet encapsulation on Layer 2 interfaces. Ethernet encapsulation is not supported on Layer 2 interfaces.

[See [encapsulation \(Logical Interface\)](#).]
- **No support for PKI operational mode commands on the Junos Limited version (MX Series routers, PTX Series routers, and SRX Series devices)**—We do not support `request`, `show`, and `clear` PKI-related operational commands on the limited encryption Junos image ("Junos Limited"). If you try to execute PKI operational commands on a limited encryption Junos image, then an appropriate error message is displayed. The `pkid` process does not run on Junos Limited version image. Hence, the limited version does not support any PKI-related operation.

Network Management and Monitoring

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
 - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral

instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

- When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

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

User Interface and Configuration

- **Support for disconnecting unresponsive NETCONF-over-SSH clients (ACX Series, PTX Series, and QFX Series)**—You can enable devices to automatically disconnect unresponsive NETCONF-over-SSH clients by configuring the `client-alive-interval` and `client-alive-count-max` statements at the **edit system services netconf ssh** hierarchy level. The `client-alive-interval` statement specifies the timeout interval in seconds, after which, if no data has been received from the client, the device requests a response. The `client-alive-count-max` statement specifies the threshold of missed client-alive responses that triggers the device to disconnect the client, thereby terminating the NETCONF session.

[See [ssh \(NETCONF\)](#).]

What's Changed in Release 21.3R1

IN THIS SECTION

- [EVPN | 155](#)
- [General Routing | 156](#)
- [Interfaces and Chassis | 157](#)
- [Junos XML API and Scripting | 158](#)
- [Layer 2 Ethernet Services | 158](#)
- [Network Management and Monitoring | 158](#)

EVPN

- **Support for displaying SVLBNH information**—You can now view shared VXLAN load balancing next hop (SVLBNH) information when you display the VXLAN tunnel endpoint information for a specified

ESI and routing instance by using `show ethernet-switching vxlan-tunnel-end-point esi esi-identifier esi-identifier instance instance svlnh` command.

- **Support for Maximum Response Time in EVPN Type 8 Routes**—Junos OS now supports the Maximum Response Time (MRT) attribute field in EVPN Type 8 Route messages. This attribute is defined in the IETF draft of IGMP and MLD Proxy for EVPN, version 13. MRT is used to synchronize the wait time before responding to IGMP messages. To maintain compatibility with devices running previous versions of Junos OS that do not support MRT, set `protocols evpn leave-sync-route-oldstyle`.

[See [evpn](#).]
- **Ethernet tag ID set to 0 for EVPN Type 6 and EVPN Type 7 routes**—For VLAN bundle and VLAN-based services, Junos OS now automatically sets the Ethernet tag ID (VLAN ID) to zero for EVPN Type 6 and EVPN Type 7 routes per RFC 7432. In earlier releases, Junos OS used the VXLAN Network Identifier (VNI) as the Ethernet tag ID. To interoperate with devices that uses the VNI as the Ethernet tag ID, set `routing-instances routing-instance-name protocols evpn smet-etag-carry-vid`.
- **Output for show Ethernet switching flood extensive**—The output for `show ethernet-switching flood extensive` now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as unicast. Previously, the output for `show ethernet-switching flood extensive` would misidentify the next-hop type as composite.

General Routing

- **Enhancement to the show chassis pic command**—You can now view additional information about the optics when you run the `show chassis pic` command. The output now displays the following additional field:

MSA Version: Multi-source Agreements (MSA) version that the specified optics is compliant to.
Values supported are: SFP+/SFP28 -- SFF-8472 (versions 9.3 - 12.3), QSFP+/QSFP28 -- SFF 8363 (versions 1.3 - 2.10), and QSFP-DD -- CMIS 3.0, 4.0, 5.0.

Previously, the `show chassis pic` command did not display this additional field.

[See [show chassis pic](#).]
- **Enhancement to the show interfaces (Aggregated Ethernet) command (ACX Series, PTX Series, and QFX Series)**—When you run the `show interfaces extensive` command for Aggregated Ethernet interfaces. You can now view following additional fields for MAC statistics : Receive, Transmit, Broadcast and Multicast packets.

[See [show chassis pic](#).]
- On PTX1K and PTX10002-60C the `show chassis hardware details` command now displays information about USB devices. In addition, information about disk drives is only displayed when the extensive switch is used with the `show vmhost hardware operational mode` command.

- **Juniper Agile Licensing (EX2300-VC, EX3400-VC, EX4300-VC, EX4400-24MP, EX4400-48MP, PTX10003, PTX10016, QFX5130-32CD, QFX5110-32Q, QFX5110-48S, QFX5120-48T, QFX5210-64C, QFX5200, and QFX5220)**—Starting from this release onwards, the Juniper Agile License Manager is deprecated. You can use the Juniper Agile Licensing Portal to activate, install, manage, and monitor licenses on Juniper Networks devices.

[See [Juniper Agile Licensing Guide](#).]

- **Validation of TCA threshold values (PTX10008)**— We've implemented immediate validation of threshold values configured in the `tca-identifier (enable-tca | no-enable-tca) (threshold number | threshold-24hrs number)` statement under the `[edit interface interface name optics-optics tca]` hierarchy level to ensure the threshold value entered is valid.

[See [optics-options](#).]

- **Renamed `verixec-check` option**—We have changed the `verixec-check` option of the `request system malware-scan` command to `integrity-check`. This update does not include any functional changes. You can use the `integrity-check` option to check whether integrity mechanisms are enabled for the Juniper Malware Removal Tool.

[See [request system malware-scan](#).]

- **Enhancement to the `request system license add terminal` command (PTX10001-36MR and vMX)**— When you run the `request system license add terminal` command. You can now view following additional fields for information: JUNOS564022985: Ignoring unknown feature .

[See [Managing vMX Licenses](#).]

.

- **New Commit check for Layer 2 Interfaces (PTX10003)**— We've introduced a commit check to prevent you from misconfiguring ethernet encapsulation on Layer 2 interfaces. Ethernet encapsulation is not supported on Layer 2 interfaces.

[See [encapsulation \(Logical Interface\)](#).]

Interfaces and Chassis

- When configuring multiple flexible tunnel interface (FTI) tunnels, the source and destination address pair needs to be unique only among the FTI tunnels of the same tunnel encapsulation type. Prior to this PR, the source and destination address pair had to be unique among all the FTI tunnels regardless of the tunnel encapsulation type.

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python op scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the device passes command-line arguments to a Python op script, it prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device prefixes a single hyphen (-) to all argument names.

[See [Declaring and Using Command-Line Arguments in Op Scripts.](#)]

Layer 2 Ethernet Services

- **Link selection support for DHCP**—We have introduced the link-selection statement at the [edit forwarding-options dhcp-relay relay-option-82] hierarchy level, which allows DHCP relay to add suboption 5 to option 82. Suboption 5 allows DHCP proxy clients and relay agents to request an IP address for a specific subnet from a specific IP address range and scope. Prior to this release, the DHCP relay dropped packets during the renewal DHCP process and the DHCP server used the leaf's address as a destination to acknowledge the DHCP renewal message.

[See [relay-option-82.](#)]

Network Management and Monitoring

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS](#) and [Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules.](#)]

- **Enhancement to the snmp mib walk command (PTX Series, QFX Series, EX Series, MX Series, SRX Series)**— The ipv6IfOperStatus field displays the current operational state of the interface. The noIfIdentifier(3) state indicates that no valid Interface Identifier is assigned to the interface. This state usually indicates that the link-local interface address failed Duplicate Address Detection. When you specify the 'Duplicate Address Detected' error flag on the interface, the new value (noIfIdentifier(3)) is displayed. Previously, the snmp mib walk command did not display the new value (noIfIdentifier(3)).
- **Changes in contextEngineID for SNMPv3 INFORMS (PTX Series, QFX Series, ACX Series, EX Series, MX Series, and SRX Series)**—Now the contextEngineID of SNMPv3 INFORMS is set to the local

engine-id of Junos devices. In earlier releases, the contextEngineID of SNMPv3 INFORMS was set to remote engine-id.

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

Known Limitations

IN THIS SECTION

- [General Routing](#) | 159
- [Infrastructure](#) | 159

Learn about known limitations in this release for PTX 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

- On PTX1000 platforms, ARP resolution failure with the IRB configuration results in packet drop. [PR1612205](#)

Infrastructure

- Image validation fails with mgd core @_rs_init, _rs_stir, _rs_stir_if_needed. Use the no-validate options, that is request system software add no-validate *image name* when upgrading software from Junos OS Release 21.1 or earlier to Junos OS Release 21.2R1 or later. [PR1568757](#)

Open Issues

IN THIS SECTION

- [General Routing | 160](#)
- [Layer 2 Ethernet Services | 161](#)

Learn about open issues in this release for the PTX 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

- On PTX Series platforms with FPC model FPC-PTX-P1-A or FPC2-PTX-P1A, you might encounter single event upset (SEU) event that might cause a linked-list corruption of the TQCHIP. The following syslog message gets reported:

```
Jan 9 08:16:47.295 router fpc0 TQCHIP1: Fatal error pqt_min_free_cnt is zero
Jan 9 08:16:47.295 router fpc0 CMSNG: Fatal ASIC error, chip TQ
Jan 9 08:16:47.295 router fpc0 TQ Chip::FATAL ERROR!! from PQT free count is zero
Jan 9 08:16:47.380 router alarmd[2427]: Alarm set: FPC color=RED, class=CHASSIS, reason=FPC 0
Fatal Errors - TQ Chip Error code: 0x50002
Jan 9 08:16:47.380 router craftd[2051]: Fatal alarm set, FPC 0 Fatal Errors - TQ Chip Error
code: 0x50002
```

The Junos OS Chassis management error handling detects such a condition, raises an alarm, and disables the affected Packet Forwarding Engine entity. To recover this Packet Forwarding Engine entity, restart the FPC. Contact your Juniper Networks support representative if the issue persists even after the FPC restarts. [PR1254415](#)

- The Next Generation Routing Engine (NG-RE) with models RE-S-X6-64G, RE-S-2X00x6, and RE-PTX-X8-64G on PTX Series platforms might encounter a transient system freeze of the Linux based host (VM Host) for about 20 - 35 seconds, cause protocol flaps, FPC restart, and mastership switch between Routing Engines. Because of the incorrect handling of the disk I/O commands, a disk I/O

timeout is reported and the system will recover by resetting the solid-state drives (SSD) channel. The system will continue to operate correctly after such an event. [PR1312308](#)

- The following log message might appear in some race conditions when NG-RE is used: kernel: interrupt storm detected on "irq11: "; throttling interrupt source [PR1386306](#)
- On Junos PTX Series platforms, the J-Flow service might not report the accurate throughput rate. This issue is seen when there is high sampled traffic rate with low flow cache hit ratio. [PR1502645](#)
- Flapping might be observed on channelized ports of PTX Series routers during ZTP, when one of the ports is disabled on the supporting device. [PR1534614](#)
- The Socket to sflowd closed error comes up when the ukern socket to sflowd daemon (server) is closed. The error is rectified by itself as the client successfully reestablishes the connection in the subsequent attempts. When these errors are consistent, it indicates a communication issue between sflowd and the sFlow running on the FPC. [PR1538863](#)
- On PTX Series platforms, when the inline J-Flow is configured and high sampling rate (more than 4000 per second) is set, a high CPU utilization might be observed. This might impact traffic analysis and billing. [PR1569229](#)
- Copying files to /tmp/ causes a huge JTASK_SCHED_SLIP. Copy files to /var/tmp/ instead. [PR1571214](#)
- On PTX1000 and PTX10002-60C platforms, file permissions for /var/db/scripts files are changed after reboot. This might impact scripts running on the box. [PR1583591](#)
- When a congestion is on the link where telemetry streams are connected, then in a race condition, na-grpcd core files are generated. This impacts the telemetry service as the na-grpcd will take a minute to come back online. [PR1587956](#)
- When the interface transitions from down to up, the carrier transition counter value of a particular interface can be incorrect when the peer interface takes longer time to come up. Configuring the hold-time for up and down helps to resolve. [PR1601946](#)
- Under MAC statistics, the output-mac-control-frames and the output-mac-pause-frames do not increment. [PR1610745](#)

Layer 2 Ethernet Services

- It is observed rarely that issuing the request system zeroize does not trigger ZTP. A simple workaround is to reinitiate ZTP. [PR1529246](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 162](#)
- [Resolved Issues: 21.3R1 | 164](#)

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

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

Resolved Issues: 21.3R2

IN THIS SECTION

- [General Routing | 162](#)
- [Layer 2 Ethernet Services | 163](#)
- [MPLS | 163](#)
- [Platform and Infrastructure | 163](#)
- [Routing Protocols | 163](#)

General Routing

- High FPC CPU utilization might be seen on PTX10002-60C routers. [PR1585728](#)
- IS-IS adjacency does not come up through TCC Layer 2 circuit. [PR1590387](#)
- High FPC CPU utilization might be intermittently observed if you receive a great number of NS/NA messages. [PR1600318](#)
- On PTX10002-60C routers, after upgrading, configured firewall filters might be applied on incorrect interfaces. [PR1602292](#)
- The FPC is not fully offline after the FPC BAD_VOLTAGE fault is reported. [PR1602556](#)

- Packet loss might be observed on a filter-based GRE deployments. [PR1603453](#)
- Traffic loss might be seen on the device due to the continuous errors happening on fabric healing process (FHP) phase-1. [PR1603499](#)
- The MACsec session might be dropped due to one way congestion. [PR1611091](#)
- Line cards might be unstable due to the continuous growing memory usage of evo-cda-bt app. [PR1614952](#)
- The rasd processes memory leak triggered by hardware memory errors on VMHost platforms. [PR1615488](#)
- Slow memory leak (32 bytes each time) of rpd might be seen. [PR1616065](#)
- Memory leak might be seen when LLDP is configured. [PR1617151](#)
- The performance of J-Flow service might be impacted on PTX Series platforms. [PR1617932](#)
- Traffic loss might be observed with some MPLS labels in multipath BGP scenarios. [PR1618507](#)
- The EAPoL packets over l2circuit might get dropped at the tunnel start. [PR1628196](#)
- The rpd process generates core file with the warm-standby configurations due to reference counting issues. [PR1631871](#)
- The SPMB might crash immediately after a switchover. [PR1637950](#)

Layer 2 Ethernet Services

- The aggregated Ethernet interface remains up instead of down on deleting loopback and ae-interface IP on neighbor while verifying BFD sessions on a router. [PR1640240](#)

MPLS

- The LDP does not support policy import with the rib-groups. [PR1611081](#)

Platform and Infrastructure

- On PTX Series platforms, vmcore on both the routing engines might be reported due to mbuf corruption. [PR1602442](#)

Routing Protocols

- The rpd process crash might be seen with telemetry used setup. [PR1607667](#)

- Delay in adding or removing static routes from the router. [PR1612173](#)
- Undesired protection path might get selected for some destination prefixes. [PR1614683](#)
- The rpd process might crash and restart when NSR is enabled. [PR1620463](#)
- The rpd process might crash after clearing the IS-IS database. [PR1631738](#)

Resolved Issues: 21.3R1

IN THIS SECTION

- [EVPN | 164](#)
- [Forwarding and Sampling | 164](#)
- [General Routing | 165](#)
- [Infrastructure | 166](#)
- [Interfaces and Chassis | 167](#)
- [Juniper Extension Toolkit \(JET\) | 167](#)
- [MPLS | 167](#)
- [Multicast | 167](#)
- [Network Management and Monitoring | 167](#)
- [Platform and Infrastructure | 167](#)
- [Routing Policy and Firewall Filters | 167](#)
- [Routing Protocols | 168](#)
- [User Interface and Configuration | 168](#)

EVPN

- EVPN option is missing under routing-instances *routing-instance-name* protocols hierarchy level. [PR1581821](#)

Forwarding and Sampling

- User-defined ARP policer is not applied on aggregated Ethernet interface until firewall process is restarted. [PR1528403](#)

General Routing

- Routing Engine switchover does not work as expected while solid-state drive (SSD) failure occurs. [PR1437745](#)
- Add Python 3.x modules that are missing from the library. [PR1508626](#)
- The VM host platforms might get crashed continuously after performing upgrade or downgrade action and booting up with the new image. [PR1544875](#)
- The device might run out of service post GRES or unified ISSU. [PR1558958](#)
- Upgrading PTX1000 platforms with unified SSDs (2x32G SSD) might result in boot loop in certain scenario. [PR1571275](#)
- Difference in the leaf names in sensor output. [PR1571502](#)
- Channelized ports on PTX10002 platforms might drop traffic. [PR1575742](#)
- Mirrored packets get corrupted when a filter is applied with the port-mirror and discard action. [PR1576914](#)
- TACACS traffic might be dropped. [PR1578579](#)
- The IS-IS packets might get corrupted on the provider edge device over the Layer 2 circuit tunnel. [PR1580047](#)
- PTX Series routers might drop traffic. [PR1580211](#)
- The FEC91 mode might not get enabled automatically for QSFP28-SR4 SFP used on WAN interface. [PR1582200](#)
- Node locked license addition fails. [PR1582704](#)
- Add missing leaves of transceiver/state in the Junos telemetry interface. [PR1583076](#)
- On PTX1000 and PTX10002-60C platforms, file permissions are changed for /var/db/scripts files after reboot. [PR1583591](#)
- The show chassis clocks output shows the following error: error: the chassis-control subsystem is not running. [PR1583715](#)
- The packets might be dropped by Packet Forwarding Engine of the PTX5000 platforms after changing the queue of IEEE-802.1ad classifier on FPC-PTX-P1-A or FPC2-PTX-P1A. [PR1584042](#)
- The FPC resource usage increases when certain packets are processed which are being VXLAN encapsulated. [PR1584197](#)
- LACP over MACsec LC (LC1105) does not come up. [PR1585478](#)

- The Failed to get pechip handle for chip 0 and prds_encap_sample_flood_lpbk_desc_install: Egress NH descriptor install OK for Flabel 7808 errors are seen during device bring up. [PR1585594](#)
- The following error message is seen on certain scenarios when rpd process restart or GRES when NSR enabled: RPD_KRT_KERNEL_BAD_ROUTE. [PR1586466](#)
- There might be higher latency in traffic flow than configured or default value. [PR1588514](#)
- The jsd process might crash in a rare condition in a telemetry scenario. [PR1589103](#)
- An FPC heap memory leak might be triggered by certain flowspec route operations which can lead to an FPC crash. [PR1589133](#)
- On PTX3000 and PTX5000 platforms, 40G and 100G interfaces might get stuck down after link flaps. [PR1589170](#)
- Traffic loss might be observed post changing SAK keys. [PR1591432](#)
- On PTX10008 platforms, sFlow sample-rate configuration greater than 16000000 is not supported. [PR1592788](#)
- Node name must not be attached to the system host name under LLDP. [PR1593991](#)
- On PTX1000 platforms, sFlow data (for example: inner VLAN and outer VLAN value, forwarding-class, and DSCP value) is not exported while checking from server flow records at the collector for ingress sampling. [PR1598263](#)
- CRC errors increase continuously after interface flap. [PR1600768](#)
- Traffic might get silently dropped and discarded due to the RS Fatal error on FPC-PTX-P1-A, FPC2-PTX-P1A, FPC-SFF-PTX-P1-A, and FPC-SFF-PTX-T. [PR1600935](#)
- The I2circuit packets with PVST and RPVST destination multicast MAC might get dropped. [PR1601360](#)
- The IPv6 traffic might get impacted on the PTX platforms when an IPv6 route resolves over a dynamic tunnel. [PR1602007](#)
- Packet loss might be seen on the filter based GRE deployments. [PR1603453](#)
- Link flaps might be observed momentarily on PTX5000 platforms. [PR1606008](#)

Infrastructure

- The default-address-selection statement might not work. [PR1570552](#)

Interfaces and Chassis

- The resiliencyd.re.re0 cores file are generated when executing cminfra scripts. [PR1578822](#)
- Junos telemetry interface optics sensor's alarm data type changed from bool_val to str_val. [PR1580113](#)

Juniper Extension Toolkit (JET)

- GRPC connections stuck on ESTABLISHED with no active collector. [PR1592542](#)

MPLS

- Sub-optimal routing issues might be seen in case where LDP routes with multiple next hops. [PR1582037](#)
- The LDP replication session might not get synchronized when the dual-transport is enabled. [PR1598174](#)
- VPLS connection might get down if the dual-transport statement is configured. [PR1601854](#)

Multicast

- Multicast traffic in an MVPN setup might get dropped and discarded silently on some PTX platforms acting as transit LSR. [PR1555274](#)

Network Management and Monitoring

- On PTX10008 platforms, syslog does not log information on IPv4 after upgrade. [PR1611504](#)

Platform and Infrastructure

- Upon receipt of specific sequences of genuine packets destined to the device, the kernel will crash and restart. [PR1557881](#)
- FPC might crash in a scaled firewall configuration. [PR1586817](#)

Routing Policy and Firewall Filters

- BGP route preference using PBR is not applied to all the routes when CCNH inet6 is enabled. [PR1596436](#)

Routing Protocols

- The unexpected CSPF link down or deleted events on LSPs are seen. [PR1576818](#)
- BGP session carrying VPNv4 prefix with IPv6 next hop might be dropped. [PR1580578](#)
- The rpd process might crash in certain IS-IS scenario. [PR1583484](#)
- The rpd process might crash when the configured record-lifetime for BGP RPKI session is less than the hold-time. [PR1585321](#)
- The rpd process might crash in a BGP multipath scenario if the interface for a single hop EBGP peer goes down. [PR1589141](#)
- BGP egress-TE routes lose to BGP routes using the same protocol preference. [PR1593332](#)

User Interface and Configuration

- The routing policy in normal-mode does not revert back once the network-services mode is changed to network-services enhanced mode. [PR1587174](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R2 documentation for PTX Series routers.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading to Release 21.3 | 169](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 171](#)
- [Upgrading a Router with Redundant Routing Engines | 172](#)

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 21.3

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 21.3R2:

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-
x86-64-21.3R2.9.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-
x86-64-21.3R2.9-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 21.3 `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 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](#).

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

- [What's New | 173](#)
- [What's Changed | 177](#)
- [Known Limitations | 182](#)
- [Open Issues | 184](#)
- [Resolved Issues | 189](#)
- [Documentation Updates | 202](#)
- [Migration, Upgrade, and Downgrade Instructions | 202](#)

These release notes accompany Junos OS Release 21.3R2 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

- [What's New in 21.3R2 | 174](#)
- [What's New in 21.3R1 | 174](#)

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

What's New in 21.3R2

There are no new features or enhancements to existing features in Junos OS Releases 21.3R2 for QFX Series.

What's New in 21.3R1

IN THIS SECTION

- [Hardware | 174](#)
- [EVPN | 175](#)
- [IP Tunneling | 176](#)
- [Routing Policy and Firewall Filters | 176](#)
- [Routing Protocols | 176](#)
- [Additional Features | 177](#)

Hardware

- **Support for transceivers (QFX5210, QFX5120, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.3R1, the QFX5210, QFX5120, QFX10008, and QFX10016 switches support these transceivers:
 - JNP-100G-2X50G-1M, JNP-100G-2X50G-3M (QFX5120-32C switches)
 - JNP-100G-2X50G-1M, JNP-100G-2X50G-3M (QFX5210-64C switches)
 - QSFP-100G-DR and QSFP-100G-FR transceivers (QFX5210-64C switches)
 - QSFP-100G-DR and QSFP-100G-FR transceivers (QFX5120-48YM switches)
 - QFX-QSFP-40G-ESR4 support (QFX10008 and QFX10016 switches with the QFX10000-30C line card)

[See [Hardware Compatibility Tool](#).]

EVPN

- **DHCP smart relay in an EVPN-VXLAN deployment (QFX5110, QFX5120, QFX5130, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.3R1, we support DHCP smart relay in an EVPN-VXLAN deployment. DHCP smart relay provides redundancy and resiliency to DHCP relay. It allows the relay agent to use multiple IP addresses as the gateway address when forwarding client requests to a DHCP server.

[See [DHCP Smart Relay for EVPN-VXLAN](#) DHCP Smart Relay for EVPN-VXLAN.]

- **Disable MAC learning on VXLAN interfaces (QFX5110 and QFX5120-48Y)**—Starting in Junos OS Release 21.3R1, you can disable MAC learning in a VXLAN. By default, MAC learning is enabled, and the VTEPs (VXLAN tunnel endpoints) learn the MAC addresses of:

- Remote hosts from the VTEPs on the remote VTEP list
- Local hosts from the local access interfaces

After the VTE learns the MAC address of a host, it adds the address to the Ethernet switching table. When you disable MAC learning on specific physical interfaces or VLAN interfaces in a VXLAN, the VTEPs are unable to learn the source and destination MAC addresses. Instead, the VXLAN receives a flood of packets that the device sends to any destination addresses.

-

- **Layer 3 VXLAN gateway support in EVPN-VXLAN fabrics using a RIOT loopback port (QFX5210)**—Starting in Junos OS Release 21.3R1, you can configure a QFX5210 switch as a Layer 3 VXLAN gateway for unicast traffic in an EVPN-VXLAN edge-routed bridging overlay fabric. QFX5210 switches require a special intermediary port for routing in and out of VXLAN tunnels (RIOT). You configure the RIOT port as a loopback LAG bundle that enables inter-VLAN routing with VXLAN tunnel initiation or termination. The RIOT loopback LAG port must be a member of all VXLAN VLANs with IRB interfaces. This feature supports:

- Only MAC-VRF routing instances with either VLAN-based or VLAN-aware bundle service types.
- Enterprise-style interface configuration.
- EVPN asymmetric Type 2 routes and EVPN Type 5 routes.

[See [Using a RIOT Loopback Port to Route Traffic in an EVPN-VXLAN Network](#).]

- **Seamless EVPN-VXLAN stitching with MAC-VRF routing instances (QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.3R1, we support seamless stitching of unicast routes across EVPN-VXLAN data centers through a WAN using MAC VRF routing instances. You can use this feature between data centers (data center interconnect [DCI]) or between points of delivery (PODs) within a data center. The EVPN control plane stitches the EVPN routes from the PODs or data centers and the WAN into a single customer-specific MAC forwarding table.

On each interconnection device, configure:

- A customer-specific EVPN instance (EVI) of type `mac-vrf`.
- Elements in the `[edit routing-instances name protocols evpn interconnect]` hierarchy in the EVI to enable the interconnection.

[See [interconnect](#) and [MAC-VRF Routing Instance Type Overview](#).]

IP Tunneling

- **Support for IP-over-IP tunnel stitching (MX Series, MX240, MX480, MX960, PTX1000, PTX10008, PTX10016, and QFX10002)**—In Junos OS Release 21.3R1, we introduce IP-over-IP tunnel stitching. You can use this feature to terminate an IP-over-IP tunnel on a device and initiate another tunnel on the same device. When a device receives the IP-over-IP packet, it de-encapsulates the outer packet header and inner packet lookup occurs. The inner IP packet header then points to another tunnel on the same device, where the same device encapsulates the packet again with another IP-over-IP header.

[See [Overview of Next-Hop-Based Dynamic Tunneling Using IP-Over-IP Encapsulation](#).]

Routing Policy and Firewall Filters

- **Support for discard interfaces (QFX-Series and PTX-Series)**—Starting in Junos OS Release 21.3R1, you can configure a discard interface for IPv4 and IPv6 traffic, which you can then use in a local policy for handling unwanted packets.

[See [Configuring Discard Interfaces](#).]

Routing Protocols

- **Check for AS match in BGP policy AS paths without using regular expressions (ACX5048, ACX5096, ACX5448, MX240, MX480, MX960, MX2008, MX10016, vMX, PTX1000, PTX5000, PTX10001, PTX10002, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, and QFX10016)**—Starting in Junos OS Release 21.3R1, you can configure BGP policies to check for an autonomous system (AS) match in an AS path without using regular expressions. The BGP policy compares the AS to an AS-list or AS-list-group and returns true if it finds a match. You can configure the BGP policy to check for a matching origin, neighbor, or transit AS. This feature provides a faster alternative to match origin, transit, and peer AS numbers than using a regular expression.

Configure this feature using the `as-path-neighbors`, `as-path-origins`, or `as-path-transits` option at the `[edit policy-options policy-statement policy-name from]` hierarchy level. For each type of match, use `(as-list | as-list-group) as-list-name/as-list-group-name` to specify the list or group of AS paths to compare the match to. Configure the AS list or AS group at the `[edit policy-options]` hierarchy level.

[See [policy-options](#) and [policy-statement](#).]

Additional Features

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

- **Precision Time Protocol (PTP) Society of Motion Picture and Television Engineers (SMPTE) media profile and the enterprise profile** (QFX5120-48YM)

[See [Understanding the Precision Time Protocol Enterprise Profile](#) and [Understanding the PTP Media Profiles](#).]

- **Precision Time Protocol (PTP) transparent clock** (QFX5120-48YM)

[See [Understanding Transparent Clocks in Precision Time Protocol](#).]

- **RPM and TWAMP** (QFX10000 line of switches)

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

- **Seamless EVPN-VXLAN stitching** (QFX10002-60C)

[See [interconnect](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.3R2 | 178](#)
- [What's Changed in Release 21.3R1 | 178](#)

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

What's Changed in Release 21.3R2

IN THIS SECTION

- [Network Management and Monitoring | 178](#)

Network Management and Monitoring

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
 - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
 - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
 - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

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

What's Changed in Release 21.3R1

IN THIS SECTION

- [Class of Service \(CoS\) | 179](#)
- [EVPN | 179](#)
- [General Routing | 180](#)
- [Interfaces and Chassis | 180](#)
- [Junos XML API and Scripting | 180](#)
- [Layer 2 Ethernet Services | 181](#)

- Network Management and Monitoring | 181
- Platform and Infrastructure | 182

Class of Service (CoS)

- On a Layer 2 interface, use unit * to apply a classifier or rewrite rule to all of the logical units on that interface.

EVPN

- **Support for displaying SVLBNH information**—You can now view shared VXLAN load balancing next hop (SVLBNH) information when you display the VXLAN tunnel endpoint information for a specified ESI and routing instance by using `show ethernet-switching vxlan-tunnel-end-point esi esi-identifier esi-identifier instance instance svlbnh` command.
- **Community information no longer included in VRF routing table**—The QFX series switches will no longer include the inherited advertised route target communities, EVPN extended communities, or vxlan encapsulation communities for EVPN Type 2 and EVPN Type 5 routes when an IP host is added in the VRF routing table.
- **Support for Maximum Response Time in EVPN Type 8 Routes**—Junos OS now supports the Maximum Response Time (MRT) attribute field in EVPN Type 8 Route messages. This attribute is defined in the IETF draft of IGMP and MLD Proxy for EVPN, version 13. MRT is used to synchronize the wait time before responding to IGMP messages. To maintain compatibility with devices running previous versions of Junos OS that do not support MRT, set `protocols evpn leave-sync-route-oldstyle`.
[See [evpn](#).]
- **Ethernet tag ID set to 0 for EVPN Type 6 and EVPN Type 7 routes**—For VLAN bundle and VLAN-based services, Junos OS now automatically sets the Ethernet tag ID (VLAN ID) to zero for EVPN Type 6 and EVPN Type 7 routes per RFC 7432. In earlier releases, Junos OS used the VXLAN Network Identifier (VNI) as the Ethernet tag ID. To interoperate with devices that uses the VNI as the Ethernet tag ID, set `routing-instances routing-instance-name protocols evpn smet-etag-carry-vid`.
- **Output for show Ethernet switching flood extensive**—The output for `show ethernet-switching flood extensive` now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as unicast. Previously, the output for `show ethernet-switching flood extensive` would misidentify the next-hop type as composite.

General Routing

- **Juniper Agile Licensing (QFX5200-32C)** Starting from this release onwards, the QFX Series switch supports following features ?
 - **Standard:** BFD, Filters (Layer 2 and Layer 3), Layer 2 (xSTP, 802.1Q, LAG), Layer 3 (static), QoS (Layer 2 and Layer 3), and SNMP
 - **Advanced 1:** Standard features, BGP, IS-IS, FBF, VRRP, MC-LAG, Layer 3 (static), GRE tunnel, OSPF, RIP, sFlow, and Virtual Chassis
 - **Advanced 2:** Advanced 1 features, CFM, Q-in-Q, VXLAN, PCEP, ESI-LAG, Timing, Ethernet OAM, EVPN-VXLAN, IGMP version 1, IGMP version 2, and IGMP version 3, PIM, and Multicast Listener Discovery (MLD) version 1 or version 2
 - **Premium:** Advanced 2 features, Layer 3 VPN, LDP, RSVP, Layer 2 circuit, EVPN-MPLS, Segment routing, MPLS, and MACsec

See [Flex Software License for QFX Series Switches and](#)

- **Juniper Agile Licensing (EX2300-VC, EX3400-VC, EX4300-VC, EX4400-24MP, EX4400-48MP, PTX10003, PTX10016, QFX5130-32CD, QFX5110-32Q, QFX5110-48S, QFX5120-48T, QFX5210-64C, QFX5200, and QFX5220)**—Starting from this release onwards, the Juniper Agile License Manager is deprecated. You can use the Juniper Agile Licensing Portal to activate, install, manage, and monitor licenses on Juniper Networks devices.

[See [Juniper Agile Licensing Guide](#).]

Interfaces and Chassis

- When configuring multiple flexible tunnel interface (FTI) tunnels, the source and destination address pair needs to be unique only among the FTI tunnels of the same tunnel encapsulation type. Prior to this PR, the source and destination address pair had to be unique among all the FTI tunnels regardless of the tunnel encapsulation type.

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python op scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the device passes command-line arguments to a Python op script, it prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device prefixes a single hyphen (-) to all argument names.

[See [Declaring and Using Command-Line Arguments in Op Scripts](#).]

Layer 2 Ethernet Services

- **Link selection support for DHCP**—We have introduced the `link-selection` statement at the `[edit forwarding-options dhcp-relay relay-option-82]` hierarchy level, which allows DHCP relay to add suboption 5 to option 82. Suboption 5 allows DHCP proxy clients and relay agents to request an IP address for a specific subnet from a specific IP address range and scope. Prior to this release, the DHCP relay dropped packets during the renewal DHCP process and the DHCP server used the leaf's address as a destination to acknowledge the DHCP renewal message.

[See [relay-option-82](#).]

Network Management and Monitoring

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS](#) and [Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules](#).]

- **Enhancement to the `snmp mib walk` command (PTX Series, QFX Series, EX Series, MX Series, SRX Series)**—The `ipv6IfOperStatus` field displays the current operational state of the interface. The `noIfIdentifier(3)` state indicates that no valid Interface Identifier is assigned to the interface. This state usually indicates that the link-local interface address failed Duplicate Address Detection. When you specify the 'Duplicate Address Detected' error flag on the interface, the new value (`noIfIdentifier(3)`) is displayed. Previously, the `snmp mib walk` command did not display the new value (`noIfIdentifier(3)`).
- **Changes in `contextEngineID` for SNMPv3 INFORMS (PTX Series, QFX Series, ACX Series, EX Series, MX Series, and SRX Series)**—Now the `contextEngineID` of SNMPv3 INFORMS is set to the local engine-id of Junos devices. In earlier releases, the `contextEngineID` of SNMPv3 INFORMS was set to remote engine-id.

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

- **Change in behavior of SNMP MIB object `ifAlias`**—SNMP MIB object `ifAlias` now shows the configured interface alias. In earlier releases, `ifAlias` used to show configured interface description.

Platform and Infrastructure

- **Enhancement to the `show chassis pic` command**—You can now view additional information about the optics when you run the `show chassis pic` command. The output now displays the following additional field:

MSA Version: Multi-source Agreements (MSA) version that the specified optics is compliant to. Values supported are: SFP+/SFP28 -- SFF-8472 (versions 9.3 - 12.3), QSFP+/QSFP28 -- SFF 8363 (versions 1.3 - 2.10), and QSFP-DD -- CMIS 3.0, 4.0, 5.0.

Previously, the `show chassis pic` command did not display this additional field.

[See [show chassis pic](#).]

- **Enhancement to the `show interfaces (Aggregated Ethernet) command (ACX Series, PTX Series, and QFX Series)`**—When you run the `show interfaces extensive` command for Aggregated Ethernet interfaces. You can now view following additional fields for MAC statistics : Receive, Transmit, Broadcast and Multicast packets.

[See [show chassis pic](#).]

Known Limitations

IN THIS SECTION

- [General Routing | 182](#)
- [Infrastructure | 183](#)

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 can hang while trying to acquire the SMP IPI lock while rebooting when it is running as a VM on Linux and QEMU hypervisor. [PR1385970](#)

- Error logs are expected when routes point to the target next hop, which in turn point to hold next hops. These error logs are present for a short time. Later, when the next hop changes from a hold next hop to valid next hop, unicast next hops will be walked again and updated with the appropriate weight and reroute counters, and no more error logs will be seen. [PR1387559](#)
- On QFX10000 line of switches, the analyzer does not mirror after adding the child member to an aggregated Ethernet interface. [PR1417694](#)
- Changing the scaled firewall profiles on the fly does not release the TCAM resources as expected. [PR1512242](#)
- On QFX5200 and QFX5100 switches with the IP-IP tunnel feature, the `show dynamic-tunnels database statistics` command output shows extra packets counts. That is, sampled packets when sFlow is enabled. [PR1555922](#)
- On QFX5000, in EVPN_VXLAN deployment, BUM (Broadcast, Unknown Unicast, and Multicast) traffic replication over VTEP might send out more packets than expected. [PR1570689](#)
- On QFX5120 switches, IRACL filters might not be able to match on VXLAN tunnel terminated packets. [PR1594319](#)
- On QFX5100 switches, the overall device utilization and FPC CPU utilization might be high in case of 4093 lrb with full port density (32/24). It might differ by maximum 4-5 percent compare to the same system having very less port density (1 or 2 ports). Some of the FPC threads takes more CPU in such scenario (for example, Ethernet and QSFP). [PR1595029](#)
- sFlow in an EVPN VXLAN IPv4 underlay, outgoing interface (OIF) will be reported as zero for ingress sampling when packet goes out through ECMP next hops. [PR1608121](#)

Infrastructure

- To upgrade to Junos OS Release 21.2R1, you need to include the `no-validate` option when issuing the upgrade command.

Junos OS releases prior to 20.4R1 do not support the `no-validate` option with unified ISSU. In order to upgrade from an older release to Junos OS Release 21.2R1 with unified ISSU, you must first upgrade to a release that supports the `no-validate` option for unified ISSU, such as Junos OS Release 20.4R1. [PR1568757](#)
- Junos OS Release 21.1 and earlier are running on FreeBSD version 11 whereas from Junos OS Release 21.2 onward, the FreeBSD version is 12. Software upgrade to Junos OS Release 21.2 or later from Junos OS Release 21.1 or earlier will mandatorily need CLI configuration statement `no-validate` during software image upgrade process. [PR1586481](#)

Open Issues

IN THIS SECTION

- General Routing | [184](#)
- EVPN | [187](#)
- Interfaces and Chassis | [188](#)
- Layer 2 Features | [188](#)
- Layer 2 Ethernet Services | [188](#)
- Platform and Infrastructure | [188](#)
- Routing Protocols | [188](#)

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

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

General Routing

- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. [PR1362609](#)
- Unified ISSU might fail from Junos OS Release 17.2X75-D43.2 to some target versions on QFX5200 platforms. And dcpfe crash might be seen. [PR1438690](#)
- The rpd process might crash if the BGP route gets resolved over the same prefix protocol next hop in the inet.3 table that has both the RSVP and LDP routes. [PR1458595](#)
- VXLAN VNI (multicast learning) scaling on QFX5110 switches traffic issue is seen from VXLAN tunnel to Layer 2 interface. [PR1462548](#)
- On QFX5000 switches with `instance-import`, deleting route which has next-table used might result in unexpected route next-op. [PR1477603](#)
- When you run the command, `show pfe filter hw filter-name filter name`, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. [PR1495712](#)

- On Junos QFX platforms, the Jflow service might not report the accurate throughput rate. This issue is seen when there is high sampled traffic rate with low flow cache hit ratio. [PR1502645](#)
- FIPS mode is not supported. [PR1530951](#)
- On QFX5100 line of switches that does not run the QFX-5E codes (non TVP architecture), when you install the image with the third party SDK upgrade (6.5.X), the CPU utilization might go up by around 5 percent. [PR1534234](#)
- The **Socket to sflowd closed** error comes up when the ukern socket to sflowd daemon (server) is closed. The error is rectified by itself as the client successfully reestablishes the connection in the subsequent attempts. When these errors are consistent, it indicates a communication issue between sflowd and the sFlow running on the FPC. [PR1538863](#)
- In an EVPN-VXLAN scenario, vmcore files are generated on primary and backup Routing Engines with Layer 2 or Layer 3 multicast configuration. [PR1539259](#)
- 100G AOC from third party does not come up after multiple reboots. It recovers after interface enable or disable. [PR1548525](#)
- On QFX5100-48S switches, the interface might remain in down state after loading the QFX 5E Series image on the device. This issue is only observed with 1G optics (SFP-SX and SFP-LX10) and when the auto-negotiation setting is enabled. The traffic through the affected interface will be lost. [PR1554098](#)
- 5M DAC connected between QFX10002-60C and MX2010 platforms does not link up. But with 1M and 3M DAC, interoperability works as expected. Also, it is to be noted that connection between QFX10002-60C and ACX or traffic generator works seamlessly with the same 5M DAC. [PR1555955](#)
- To avoid the additional interface flap, interface hold time needs to be configured. [PR1562857](#)
- Unable to execute python or shell scripts in flex mode. Starting in Junos OS Release 21.1R1 release, Junos OS ships with python3 (python2 is no longer supported). In ZTP process, if a python script is being downloaded, ensure that the python script follows python3 syntax (there are certain changes between python2 and python3 syntax). Also, so far (that is, until Junos OS Release 20.4R1), the python script had `#!/usr/bin/python` as the first line (that is, the path of the python interpreter). The same needs to be changed to `#!/usr/bin/python3` from Junos OS Release 21.1R1. [PR1565069](#)
- The chassisd logs are flooded with the `pic_create_ifname: 0/0/0 pic type F050 not supported` error messages for every port that is connected. This happens repeatedly in a few seconds. [PR1566440](#)
- In a mixed QFX5100 VCF setup, duplicate traffic might be observed for some Layer 3 multicast traffic streams. [PR1568152](#)
- On QFX5000 switches, Broadcast, Unknown Unicast, and Multicast (BUM) traffic replication over VTEP out more packets than expected and there seems to be a loop. [PR1570689](#)

- The OSPF session over IRB might not come up in an EVPN-VXLAN scenario. [PR1577183](#)
- On QFX5100 switches, while checking the DHCP smart relay over IRB interfaces, the renew-ack might not be seen in the DHCP client. [PR1581025](#)
- In a fully loaded device, firewall programming fails at times due to scaled prefix configuration with more than 64800 entries. [PR1581767](#)
- When physical loopback is used and both the ports are with EP style in the same RSPAN VLAN, it might lead to flooding. [PR1581876](#)
- On all Junos OS platforms, when there is a congestion on the link where telemetry streams are connected, in a race condition, na-grpcd core files are generated. This impacts the telemetry service as the na-grpcd will take a minute to come back online. [PR1587956](#)
- On QFX5000 line of switches, the FPC or dcpfe process might go into a very uncommon state when multiple third-party counter (bcmCNTR) threads are running or spawned in FPC. This state causes the dcpfe process to crash or the FPC to reboot. The purpose of bcmCNTR is to poll statistics from hardware. [PR1588704](#)
- On QFX3500, QFX3600, QFX5100, QFX5110, QFX5120, QFX5130, QFX5200, QFX5210, and QFX5220; switches with the third-party chip as Packet Forwarding Engine, if IS-IS is enabled on an integrated routing and bridging (IRB) interface and the maximum transmission unit (MTU) size of the IRB interface is configured with a value great than 1496 bytes, the IS-IS hello (IIH) PDUs with jumbo frame size (that is great than 1496 bytes) might be dropped and not sent to the IS-IS neighbors. [PR1595823](#)
- Pim VXLAN does not work on the TD3 chipsets that enable the VXLAN flexflow. [PR1597276](#)
- On QFX Series switches, the dcpfe process or FPC might crash during boot time if you reboot the devices. [PR1597479](#)
- On QFX5200 switches, dcpfe core files are generated while testing unified ISSU. [PR1600807](#)
- The convergence time degradation is seen in IS-ISv6, OSPFv2, and OSPFv3 when comparing convergence time with Junos OS Release 21.1R1.5. [PR1602334](#)
- On QFX10008 switches, the system reboot takes approximately 9 minutes for FPCs to come online after system reboot command is issued. [PR1605002](#)
- On QFX5100 switches, generate an optical power after detaching and attaching the QSFP on disabled interface. [PR1606003](#)
- On QFX5110 and QFX5120 switches, when you configure an EP and SP style logical interface on same physical interface with native VLAN on SP style logical interface in an EVPN-VXLAN scenario, traffic drop or unexpected behavior in traffic might be seen. [PR1606106](#)

- On QFX10000 line of switches, service provider style configuration is not supported with sFlow. [PR1608360](#)
- On QFX10002-60C switches under MAC statistics, the output-mac-control-frames and the output-mac-pause-frames do not increment. [PR1610745](#)
- On QFX5100 Virtual Chassis, when 118 (max) lag groups are configured, then there might be traffic loss of a few packets intermittently. [PR1611162](#)
- On QFX5120-48Y switches, when scaled and baseline configurations are loaded multiple times one after other without much waiting time in between, then the traffic or protocols on pure Layer 3 interfaces might behave in an undefined or unexpected manner. [PR1612973](#)
- On QFX10002, QFX10008, and QFX10016 switches, on scaling more than 80,000 ARP/NDP, the **prds_jpf_nh_token_change: Token change failed for rnh** error messages get generated. [PR1616224](#)
- CLI command is not supported by QFX10008 and QFX10016 platforms. Hence disabling the same. [PR1635812](#)
- In multihoming EVPN-VXLAN environment with QFX5000 series platforms (QFX5110, QFX5120, QFX5200, QFX5210, and QFX5220) working as PE devices, packets to some destinations might be dropped in ingress PE, due to a VP-LAG (Virtual Port LAG) programming issue in PFE (Packet Forwarding Engine) in specific cases. [PR1644152](#)

EVPN

- End-hosts might not communicate via EVPN-VXLAN domain after ESI failover. This issue affects QFX5000 platforms only. [PR1584595](#)
- With the shared-tunnels enabled, the AR tunnels do not get formed on the DC-GW for the MAC-VRF instances. [PR1584790](#)
- Modifying the I-ESI value is traffic effecting event. If this must be done then follow the below steps in order to avoid I-ESI modification issue.
 - 1) Deactivate interconnect stanza for the routing-instance in question.
 - 2) Modify the I-ESI value.
 - 3) Activate the interconnect stanza.[PR1600600](#)
- MAC-IP that moves across Layer 2 DCI does not get updated in the MAC-IP table of the GW nodes for VLANs that have translate VNI configuration. [PR1610432](#)

Interfaces and Chassis

- After restart of ICCP service, the `show iccp` command takes more than 20s to display the **client-name** information. [PR1618987](#)

Layer 2 Features

- If the access-side interfaces are 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 a 20-50 ms traffic drop on the existing logical interface. [PR1367488](#)

Layer 2 Ethernet Services

- It is observed rarely that issuing the `request system zeroize` command does not trigger ZTP. As a workaround, reinitiate the ZTP. [PR1529246](#)
- The DHCP client configuration is coming from two places, i.e AIU script and vsdk sandbox. The DHCP client configuration coming from AIU script has the serial ID in vendor ID whereas the default configuration from sandbox doesn't have. There is no impact on functionality or service. [PR1601504](#)

Platform and Infrastructure

- The `commit synchronize` command fails because the kernel socket gets stuck. [PR1027898](#)
- Arrival rates do not appear at the system level when you configure the `global-disable`. [PR1438367](#)
- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect ASIC programming. [PR1530160](#)

Routing Protocols

- In a Virtual Chassis or Virtual Chassis fabric scenario, inconsistent MCSNOOPD core file is seen when the `igmp-snooping` configuration is removed. [PR1569436](#)

- When the configuration statement `accept-remote-source` under PIM is removed, the PIM SG entries might not be updated with the correct RPF. Clearing of the states would take care of the issue. This is day-1 behavior. [PR1593283](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 189](#)
- [Resolved Issues: 21.3R1 | 195](#)

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.

Resolved Issues: 21.3R2

IN THIS SECTION

- [General Routing | 190](#)
- [Class of Service \(CoS\) | 193](#)
- [EVPN | 193](#)
- [High Availability \(HA\) and Resiliency | 194](#)
- [Infrastructure | 194](#)
- [Layer 2 Ethernet Services | 194](#)
- [MPLS | 194](#)
- [Platform and Infrastructure | 194](#)
- [Routing Policy and Firewall Filters | 194](#)
- [Routing Protocols | 195](#)

General Routing

- Multiple entries to vlan-id-list might not work in EVPN-VXLAN scenario. [PR1564403](#)
- The na-grpcd process might generate core files during the longevity tests. [PR1565255](#)
- On the QFX10K2-60C line of switches, the disk missing alarm does not get generated. [PR1573139](#)
- When soft loopback port and analyzer configurations are committed together, hardware might not get programmed with the analyzer. This issue is not seen when physical loopback is used to achieve the same. [PR1581542](#)
- On QFX5000 line of switches, the show route detail command might not display the Next-hop type IPoIP Chained comp nexthop in the output. [PR1584322](#)
- On the QFX10002-60C line of switches, high FPC CPU utilization might occur. [PR1585728](#)
- The Syslog ERROR message might be seen when deactivating Bridge domains/VLANS. [PR1589138](#)
- On the QFX5210-64C line of switches, the PSU firmware upgrades through Junos OS. [PR1589572](#)
- The DCI InterVNI and IntraVNI traffic might be silently discarded in the gateway node due to the tagged underlay interfaces. [PR1596462](#)
- The mcsnoopd process might crash when you delete or add the Layer 2 forwarding configuration after ISSU. [PR1596483](#)
- During FRR, when more than one multihome interface is down, traffic might get loop for QFX5110 platforms. [PR1596589](#)
- The interface on SFP-T or SFP-SX might stop forwarding traffic. [PR1598805](#)
- Read write lock is not acquired during the sysctl invocation. The assert triggered in the interface state function call leads to go Routing Engine 1 to debug (db>) prompt. [PR1598814](#)
- The SFP-T port might stop forwarding traffic. [PR1600291](#)
- The VCP might not form adjacency after rebooting the primary FPC in VC scenario. [PR1600398](#)
- Removing and adding VC ports might cause the FPC to reboot. [PR1601557](#)
- InterDC traffic loss might occur in the MAC-VRF EVI with the **dlu.ucode.discard** trap status. [PR1601961](#)
- Under certain scaling scenarios with EVPN-VXLAN configurations, the l2ald process might be aborted and then recovered. [PR1602244](#)
- In Junos OS, specific packets over VXLAN cause FPC memory leak and ultimately reset (CVE-2022-22170). [PR1602407](#)

- On the QFX5120 line of switches, traffic gets mirrored even after deactivating the analyzer configuration. [PR1603192](#)
- Unicast DHCP packets might get flooded when you configure the DHCP relay in the non-default routing-instance. [PR1603444](#)
- Packet loss might occur on the filter-based GRE deployments. [PR1603453](#)
- The Virtual Chassis ports might remain in the Down state after you remove and add the ports. [PR1606705](#)
- FPC might crash post firewall filter configuration changes in QFX platforms. [PR1608610](#)
- An additional VLAN tag might be added for PPPoE (Point-to-Point Protocol over Ethernet) packets on QFX10016. [PR1610012](#)
- On the QFX10000 line of switches, continuous Layer 3 traffic might drop with the MC-LAG configuration. [PR1610173](#)
- MAC move or MAC flap might be triggered in the QFX5000 Series Virtual Chassis environment. [PR1610295](#)
- Inter-vlan connectivity might be lost in an EVPN-VXLAN with CRB topology. [PR1611488](#)
- Layer 3 interfaces unable to attach DSCP rewrite firewall filter on QFX5100. [PR1612587](#)
- On the QFX10002-60C line of switches, continuous FPC might crash and the dcpfe process might generate core file. [PR1612871](#)
- ARP resolution for data traffic received over Type5 might fail. [PR1612905](#)
- FPC might crash after device restart in EVPN-VXLAN scenario. [PR1613702](#)
- Removing the optical module **JNP-SFPP-10GE-T** from a port might cause certain ports to go down. [PR1614139](#)
- On the QFX5000 line of switches, the VLAN firewall filter does not get deleted in the Packet Forwarding Engine after configuration changes. [PR1614767](#)
- The l2ald process might crash in the EVPN scenario. [PR1615269](#)
- Slow memory leak (32 bytes each time) of rpd might be seen. [PR1616065](#)
- The l2cpd process generates a core file with the FIP snooping configuration on any interface. [PR1617632](#)
- The BFD session might get become nonresponsive in the Init state after l2-learning restart due to incomplete ARP resolutions. [PR1618280](#)

- Core dumps might be seen on QFX devices after configuration changes. [PR1618352](#)
- Traffic might be dropped when IRB is configured and removed from VLAN. [PR1618425](#)
- Junos OS does not support the Dot1x based firewall policers. [PR1619405](#)
- The process dcpfe might crash after performing VXLAN VNI configuration change and delete on QFX5000 series platforms. [PR1619445](#)
- Disabled VCP (Virtual chassis port) might go into the Up state after the optic is reseated. [PR1619997](#)
- High wired memory utilization might be observed if GRES is enabled. [PR1620599](#)
- Routes learned via the EVPN Type-5 route are not resolved. [PR1620627](#)
- EVPN-VXLAN type5 traffic might get failed on the spine device of QFX10000. [PR1620924](#)
- On the QFX5120 line on switches, the **tvp_is_qsfp_has_single_led ioctl call failed ret:-1** error message gets generated while loading the build. [PR1621630](#)
- LED indicator might be showing **ON** status once QSFP is removed. [PR1622580](#)
- Host generated IPv4 traffic sent over IPv6 next-hop with IRB interface might get dropped. [PR1623262](#)
- MACsec session might flap if multiple logical interfaces are created on single physical interface. [PR1624524](#)
- QFX5000 log messages, **fpc0 SRIRAM Tx VxLAN Ucast: ifd_out = vtep dst_gport is (c00000X)** so do not process pkt further. [PR1624925](#)
- Traffic loss might be observed after configuring VXLAN over IRB interface. [PR1625285](#)
- The configuration statement **no-incoming-port** is not applied after reboot on QFX10002 and QFX10008 platforms. [PR1625988](#)
- Implement **show task scheduler-slip-history** to display no of scheduler slips and last 64 slip details. [PR1626148](#)
- Routing Engine generated traffic might not be forwarded when next-hop is indirect unilist of EVPN Type 5 tunnel. [PR1627363](#)
- QFX10002-60C platform might not respond back to ICMP packets received with TTL or hop limit value of 1. [PR1627566](#)
- JDI-RCT: QFX10002 MCLAG PDT: L3 Traffic failures observed continuously with PDT mclag configuration. [PR1627846](#)

- The 802.1p BA classification might not work on mixed VC when interface has a DSCP and 802.1p classifier. [PR1628447](#)
- When DHCP smartrelay is used DHCP inform ack might be sent with broadcast address. [PR1628837](#)
- The vmhost crash might be seen in a rare condition when route addition and change. [PR1629200](#)
- Traffic might get dropped when family ethernet-switching is configured on the interface in Q-in-Q scenario. [PR1629680](#)
- On QFX5000, chassis status LED doesn't work as document described. [PR1630380](#)
- The FBF filtered VLAN traffic will not be passed properly to the forwarding routing instances over aggregated Ethernet interfaces on QFX5000 platforms. [PR1633452](#)
- Traffic loss after MAC ages. [PR1633879](#)
- The VCPs connected with the AOC cable might not come up after upgrading to 17.3 or later releases. [PR1633998](#)
- Data might not be exchanged via EVPN-VxLAN domain. [PR1635347](#)
- Traffic blackhole might be observed when STP is configured in VxLAN environment. [PR1636950](#)
- Configuring L2PT on a transit switch in a Q-in-Q environment breaks L2PT for other S-VLANs. [PR1637249](#)
- Delay might be observed for the interfaces to come up after reboot and transceiver replacement. [PR1638045](#)
- MAC-move might be observed when dhcp-security is configured. [PR1639926](#)

Class of Service (CoS)

- Transit packets from local to remote VTEP might get punted to CPU and cause DDoS events. [PR1489233](#)
- The dcpfe core might be seen in auto-channelization scenario or when SFP is plugged out. [PR1616847](#)

EVPN

- In EVPN VXLAN scenario, with the proxy-macip-advertisement statement is configured, a few ARP/ND/MAC entries might get missed. [PR1609322](#)
- The MAC-table aging timeout fails in some scenarios. [PR1612866](#)

- Multiple memory leaks might be seen leading to process rpd crash. [PR1626416](#)

High Availability (HA) and Resiliency

- Memory leaking might occur on backup Routing Engine when ksyncd is in inconsistent state and had encountered an initialization error. [PR1601960](#)

Infrastructure

- The **Host 0 Active Disk Usage Exceeded** alarm might be generated due to large files, which were already marked as deleted. [PR1601251](#)

Layer 2 Ethernet Services

- Enabling DHCP on Junos platforms might cause the router's file system storage to get filled up with log files. [PR1617695](#)

MPLS

- MPLS VPN packets drop due to missing ARP entry on PE. [PR1607169](#)
- On the QFX5000 line of switches, traffic loss occurs after the STP topology changes. [PR1616878](#)
- Traffic towards MPLS-Core is not rerouted to alternate port on QFX5000 platforms. [PR1627002](#)

Platform and Infrastructure

- IPv6 link-local traffic is getting classified to firewall host this might affect communication on IPv6 link-local addresses. [PR1600085](#)
- The packet drop might be seen on FPC on Trio based platforms. [PR1631313](#)

Routing Policy and Firewall Filters

- The interface-routes rib-group policy does not work as expected in the VxLAN scenario. [PR1537306](#)
- The rpd process might get stuck at 100% when EVPN vrf-target is enabled and after any configuration change. [PR1616167](#)

Routing Protocols

- The interface might receive multicast traffic from a multicast group which it is not interested in. [PR1612279](#)
- The wrong BGP path might get selected even when a better or preferred route is available. [PR1616595](#)
- Traffic drop will be seen when VPN labels are incorrectly allocated due to change in nexthop. [PR1617691](#)
- On the QFX10002 line of switches, the verification of BGP peer count fails after deleting the BGP neighbors. [PR1618103](#)
- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific BGP export policies. [PR1626367](#)

Resolved Issues: 21.3R1

IN THIS SECTION

- [Class of Service \(CoS\) | 195](#)
- [EVPN | 196](#)
- [Interfaces and Chassis | 196](#)
- [Layer 2 Features | 196](#)
- [Layer 2 Ethernet Services | 196](#)
- [Platform and Infrastructure | 197](#)
- [Routing Protocols | 201](#)
- [User Interface and Configuration | 202](#)

Class of Service (CoS)

- The buffer allocation for VCP ports might not get released in Packet Forwarding Engine after physically moving the port location. [PR1581187](#)
- DSCP classifier might not work properly on QFX5000 line of platforms. [PR1585361](#)
- TCP-ECN traffic might not be forwarded with high priority. [PR1585854](#)

EVPN

- The l2ald process might crash and restart with an l2ald core file generated when the global level telemetry sensor is enabled. [PR1570757](#)
- Configuring the static-mac and no-mac-learning simultaneously on the VXLAN interface causes stale MAC/IP entry in the EVPN database. [PR1576147](#)
- After device reboot in an EVPN-VXLAN setup with graceful restart, EVPN routes are not advertised to EVPN peers until rpd is up for 180 seconds. [PR1586246](#)
- Traffic loss might be seen under EVPN-VXLAN scenario when MAC-IP moves from one CE interface to another. [PR1591264](#)
- The label field for the EVPN Type 1 route is set to 1. [PR1594981](#)
- The device announces router-mac, target, and EVPN-VXLAN community to BGP IPv4 NLRI. [PR1600653](#)
- There is a steady increase in storage usage in the backup chassis when the subscriber service is enabled. [PR1605375](#)

Interfaces and Chassis

- Newly added MC-LAGs do not come up after Routing Engine switchover. [PR1583547](#)
- Removing the configuration from the interface stanza might cause the dcpfe process to crash. [PR1594356](#)

Layer 2 Features

- The DF might not forward BUM traffic on QFX5000 series switches. [PR1575976](#)
- MAC addresses learned from the MC-LAG client device might keep flapping between the ICL interface and MC-AE interface after one child link in the MC-AE interface is disabled. [PR1582473](#)
- Traffic drop might be seen on the aggregate Ethernet interface. [PR1585320](#)

Layer 2 Ethernet Services

- The DHCP client will be offline for 120 seconds after sending the DHCPINFORM message in the DHCP relay scenario. [PR1575740](#)
- DHCP relay drops packets during the DHCP renewal process. [PR1576417](#)

- The traffic received on a port in LACP detached state might be incorrectly forwarded. [PR1582459](#)
- The DHCP client might be offline for about 120 seconds after sending the DHCPINFORM message. [PR1587982](#)

Platform and Infrastructure

- Routing Engine switchover does not work as expected while solid-state drive (SSD) failure occurs. [PR1437745](#)
- On QFX5220-128C platforms, an interface might stay down for around 3 seconds after the interface is enabled or fiber is inserted. [PR1480112](#)
- Console access on backup Virtual Chassis member is not allowed. [PR1530106](#)
- Kernel crash might occur after NSSU while performing GRES. [PR1533874](#)
- The interface might not come up with 1 Gigabit optics. [PR1554098](#)
- The interface might go into blocking state impacting the traffic when link-protection switches from primary to backup. [PR1555294](#)
- The Virtual Chassis port might not come up after upgrading to 18.4R2-S4 or later releases on the QFX5100 platform. [PR1555741](#)
- On QFX Series platforms, l3static license is required though it is included in base license [PR1557631](#)
- Upon receipt of the specific sequences of genuine packets destined to the device, the kernel will crash and restart (vmcore). [PR1557881](#)
- The MAC addresses learned in a Virtual Chassis might fail due to aging out in a MAC scaling environment. [PR1558128](#)
- The Virtual Chassis fabric might not become stable. [PR1559172](#)
- On the QFX5110 line of switches, the untagged traffic routed over the native-vlan might be dropped. [PR1560038](#)
- The dcpfe process might crash after committing EVPN-VXLAN profile configuration and the ARP resolution might fail, causing traffic issues. [PR1561588](#)
- On QFX5110-32Q switches, LACP does not come up in the non-oversubscribed mode for a set of ports. [PR1563171](#)
- The rpd process might crash during boot. [PR1567043](#)
- MAC addresses might not be relearned successfully after MAC address age timeout. [PR1567723](#)

- DCI traffic loss of 100 percent is observed in transit spine devices. [PR1572238](#)
- In an EVPN-VXLAN CE interface with RSTP configuration might cause LACP or BFD issues. [PR1572504](#)
- DCPFE or FPC might crash on the QFX10000 Series platforms if the ARP MAC move happens. [PR1572876](#)
- On the QFX10008 chassis, the dcpfe process generates a core file. [PR1572889](#)
- Upgrading to Junos OS Release 20.3 or later might report a warning: requires 'l3vpn' license message on commit when a VRF instance configuration exists. [PR1575608](#)
- The dual speed supported DAC cable (100G to 4x25G splitter) might not come up on QFX5120-48Y platform. [PR1576180](#)
- On QFX5000 line of switches, control traffic might be dropped if a high rate of specific multicast traffic is received. [PR1576488](#)
- Multicast packets with TTL=1 are dropped on a VXLAN enabled interface when igmp-snooping or MLD-snooping is enabled. [PR1576775](#)
- The port might not get brought down immediately during some abnormal type of line card reboot on QFX10000 platforms. [PR1577315](#)
- TACACS traffic might be dropped. [PR1578579](#)
- The dcpfe process might crash when any interface flaps. [PR1579736](#)
- The IS-IS packet might be corrupted on the provider edge device over the I2circuit tunnel. [PR1580047](#)
- The dcpfe process crashes while checking the virtual tunnel next hop packet status. [PR1580114](#)
- DHCP packets might be dropped if the dynamic filter dyn-dhcpv4_v6_trap is applied on the interface. [PR1580352](#)
- While mapping analyzers to the channelized port, mirror might not work properly. [PR1580473](#)
- On QFX5120-32C line of switches, the following error is observed: kern.ipc.maxpipekva exceeded; see tuning error. [PR1581192](#)
- The switchover might be affected with the shared VXLAN tunnel. [PR1581524](#)
- The traffic might not be load balanced properly in an EVPN overlay-ecmp setup. [PR1582017](#)
- Some 40 Gbps ports might not be channelized successfully on the QFX5100 platforms. [PR1582105](#)
- The pciephy and firmware download is not working after migrating to 6.5.19. [PR1582244](#)

- On QFX10000 line of switches, the firewall filter logs are incorrectly populate the protocol 8847 entries. [PR1582780](#)
- The srpxfe process might crash. [PR1582989](#)
- Firewall filter is not getting programmed after deleting a large filter and adding a new one in a single commit on QFX5000 platforms. [PR1583440](#)
- The QFX5000 and QFX10000 devices might get hanged for sometime after reboot. [PR1584902](#)
- The ZTP process might cause the traffic to be dropped and discarded silently. [PR1585057](#)
- The DHCP offer packets might be dropped on spine device in a VXLAN multihoming setup. [PR1585715](#)
- Inter and intra VNI traffic might drop in spine with EVPN-VXLAN CRB configuration. [PR1586537](#)
- An FPC heap memory leak might be triggered by certain flowspec route operations which can lead to an FPC crash. [PR1589133](#)
- In an EVPN-VXLAN scenario, 50 percent traffic loss might happen. [PR1589547](#)
- FPC might crash in a scaled firewall configuration. [PR1586817](#)
- On QFX5210-64C switches, add a command line to upgrade PSU jfirmware through Junos OS. [PR1589572](#)
- When the member interface is removed from the aggregated Ethernet interface, it is not removed from mirroring in the analyzer. [PR1589579](#)
- LLDP packets drop on SP style interface for QFX devices. [PR1589702](#)
- The MPLS traffic might not be forwarded after the aggregate interface flaps on QFX5120 devices. [PR1589840](#)
- VXLAN DDoS violation might occur when you disable the port mirror analyzer output interface. [PR1590150](#)
- Virtual Chassis mastership change and connection drop might be seen after renumbering of backup member ID. [PR1590358](#)
- On QFX5120-48T platforms, after removing 1G speed on interfaces it does not come back as 10G. [PR1591038](#)
- The xSTP might not get configured when it is enabled on a interface with SP style configuration. [PR1592264](#)
- Routing Engine kernel might crash due to logical interface of the aggregated interface adding failure in Junos OS kernel. [PR1592456](#)

- The IPv4 fragmented packets might be broken if PTP transparent clock is configured. [PR1592463](#)
- MPLS traffic might get discarded on passive monitoring interface on QFX10002, QFX10008, QFX10016 switches. [PR1592693](#)
- Multiple crashes with `toe_interrupt_errors` might be observed. [PR1593025](#)
- BFD session might flap during Routing Engine switchover. [PR1593244](#)
- The `dcufe` process might crash in an EVPN-VXLAN scenario. [PR1593950](#)
- Packet drop might occur in an ECMP next hop flap scenario. [PR1594030](#)
- ARP entry might be found missing intermittently post FPC reboot. [PR1594255](#)
- The existing ECMP route traffic might be dropped if you configure a static ECMP route with the same number of next hops as the existing ECMP route. [PR1594573](#)
- The reinstallation of the Type-5 tunnels might fail in an EVPN-VXLAN scenario. [PR1595197](#)
- The `fpc0 bcm pkt reinsert failed` log written in the log messages in an aggressive way. [PR1596643](#)
- The IS-IS adjacency might fail to be formed if the MTU size of an IRB interface is configured with a value great than 1496 bytes. [PR1595823](#)
- Traffic might be dropped after backup FPC is rebooted in a Virtual Chassis scenario. [PR1596773](#)
- The interface might not be brought up when Q-in-Q is configured. [PR1597261](#)
- Deletion of MACsec configuration on a logical interface is not taking effect. [PR1597848](#)
- Socket connection drops due to keepalive timer expiration with port 33015. [PR1598019](#)
- s-Flow impacts ICMP traffic on the QFX5120-48Y switches. [PR1598239](#)
- On QFX5100, QFX5110, QFX5120, QFX5200, and QFX5210 platforms, DDoS violations might be reported incorrectly for IP multicast miss traffic (IPMCAST-MISS). [PR1598678](#)
- File permissions are changed for `/var/db/scripts` files after reboot. [PR1599365](#)
- The Layer 3 traffic gets silently dropped and discarded on the QFX10002-60C devices with IRB interface. [PR1599692](#)
- Unable to disable the management port `em1`. [PR1600905](#)
- On QFX5120-48Y switches, `dc-pfe` core file is generated while issuing the `show pfe vxlan nh-usage` command in an ERB EMC scenario with ~6000 ARP entries. [PR1601949](#)
- The IPv6 traffic might be impacted on the QFX platforms when an IPv6 route resolves over a dynamic tunnel. [PR1602007](#)

- The egress interface of the GRE tunnel is not dynamically updated when the destination to tunnel is changed. [PR1602391](#)
- FPC goes down and dcpfe core files are generated in some cases. [PR1602583](#)
- Traffic loss might be seen in an MC-LAG scenario on QFX platforms. [PR1602811](#)
- Traffic drop might be observed on QFX5000 line of platforms in a Virtual Chassis scenario when the firewall filter is configured. [PR1602914](#)
- The dot1x authentication might not work on EVPN-VXLAN enabled endpoints. [PR1603015](#)
- Packet loss might be seen on the filter based GRE deployments. [PR1603453](#)
- Duplicate packets might be seen during bringing up all the interfaces on the spine switches. [PR1604393](#)
- On QFX5210-64C platforms, the carrier transition counter does not increment on link flap after reboot. [PR1605037](#)
- MAC move might be seen between the ICL and the MC-LAG interface if you add or remove VLANs on the ICL interface. [PR1605234](#)
- Multicast streams might stop flooding in a VXLAN setup. [PR1606256](#)
- LLDP packets received on a VXLAN enabled port might be flooded unexpectedly. [PR1607249](#)
- The fxpc process might crash and generate a core dump file. [PR1607372](#)
- Ping to lo0 and IRB over type 5 fails. [PR1610093](#)
- On QFX Series Virtual Chassis might lose license. [PR1610272](#)
- MAC move or MAC flap might be triggered in the QFX5000 Series Virtual Chassis environment. [PR1610295](#)

Routing Protocols

- The remaining BFD sessions of the aggregated Ethernet interface flap continuously if one of the BFD sessions is deleted. [PR1516556](#)
- On QFX5000 line of switches, the DHCP packets in a static VXLAN scenario might be dropped. [PR1576168](#)
- Traffic loss might be observed in an EVPN-VXLAN scenario on QFX5000 line of platforms. [PR1580005](#)
- BGP sessions carrying VPNv4 prefix with IPv6 next hop might be dropped. [PR1580578](#)

- Traffic loss might be seen when IPv6 traffic forwarded by IPv4 GRE tunnel. [PR1582408](#)
- With the IGMP snooping implemented, unexpected jitter issue is seen and that might cause traffic loss. [PR1583207](#)
- The rpd process might crash after committing with the static group configured. [PR1586631](#)
- The multi hop BFD session might flap if the Request Support Information (RSI) collection command is executed. [PR1589765](#)
- BGP egress-TE routes lose to BGP routes using the same protocol preference. [PR1593332](#)
- The IPv4 static route might still forward traffic unexpectedly even when the static route configuration has already been deleted. [PR1599084](#)

User Interface and Configuration

- During rare circumstances, the mgd process might crash and generates a core file on Junos OS devices connected with Contrail Service Orchestration (CSO). [PR1569903](#)
- The system archival might not work inside routing-instance. [PR1572228](#)

Documentation Updates

There are no errata or changes in Junos OS Release 21.3R2 documentation for QFX Series switches.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrading Software on QFX Series Switches | 203](#)
- [Installing the Software on QFX10002-60C Switches | 205](#)
- [Installing the Software on QFX10002 Switches | 206](#)
- [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 | 207](#)
- [Installing the Software on QFX10008 and QFX10016 Switches | 208](#)
- [Performing a Unified ISSU | 212](#)

- [Preparing the Switch for Software Installation | 212](#)
- [Upgrading the Software Using Unified ISSU | 213](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 215](#)

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 **21.3** 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 21.3 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-x86-64-21.3-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 21.3 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-x86-64-21.3R1.9.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-x86-64-21.3R1.9.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-x86-64-21.3R1.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-x86-64-21.3R1.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-x86-64-21.3R1.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-
x86-64-21.3R1.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)

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

Performing a Unified ISSU

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

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

Perform the following tasks:

- No Link Title
- No Link Title

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

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

To verify that nonstop active routing is enabled:

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

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

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

- Enable nonstop bridging (NSB). See *Configuring Nonstop Bridging on Switches (CLI Procedure)* 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-x86-64-21.3R1.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 7: EOL and EEOL Releases

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

- [What's New | 217](#)
- [What's Changed | 223](#)
- [Known Limitations | 226](#)
- [Open Issues | 227](#)
- [Resolved Issues | 230](#)
- [Documentation Updates | 241](#)
- [Migration, Upgrade, and Downgrade Instructions | 241](#)

These release notes accompany Junos OS Release 21.3R2 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

- [What's New in 21.3R2 | 217](#)
- [What's New in 21.3R1 | 217](#)

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

What's New in 21.3R2

There are no new features or enhancements to existing features in Junos OS Releases 21.3R2 for SRX Series.

What's New in 21.3R1

IN THIS SECTION

- [Application Identification \(AppID\) | 218](#)
- [Flow-Based and Packet-Based Processing | 219](#)
- [Intrusion Detection and Prevention | 219](#)
- [J-Web | 219](#)
- [Juniper Advanced Threat Prevention Cloud \(ATP Cloud\) | 221](#)
- [Network Management and Monitoring | 221](#)
- [VPNs | 222](#)
- [Additional Features | 222](#)

Learn about new features or enhancements to existing features in this release for the SRX Series.

Application Identification (AppID)

- **First-packet classification in advanced policy-based routing (APBR) (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.3R1, APBR uses first-packet classification to identify applications in network traffic. APBR identifies applications by examining the very first packet in the traffic flow and then applies application-specific rules to forward the traffic.

With first-packet classification, you can steer the traffic accurately and efficiently over the network, optimizing network link utilization and boosting the performance.

See [[Advanced Policy-Based Routing Overview.](#)]

- **IPv6 address support in application quality of experience (AppQoE) (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.3R1, you can use IPv6 addresses in AppQoE configurations. The support includes:

- IPv6 address in overlay path configuration
- Active probing sessions using IPv6 addresses as source and destination address.
- IPv4 and IPv6 traffic from the client side
- Dual stacking of IPv4 and IPv6 on the LAN side
- IPv6 address on the LAN side for SaaS (software as a service) probing

See [[Application Quality of Experience.](#)]

- **IPv6 traffic for application-based multipath routing (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.3R1, we support application-based multipath routing in the following IPv6 use cases:

- IPv6 traffic over IPv6 tunnels
- Application-based multipath routing over direct IPsec tunnels without GRE for IPv6 traffic
- Application-based multipath routing over direct GRE tunnels without IPsec for IPv6 traffic
- Application-based multipath routing over MPLS-over-GRE-over-IPsec for IPv6 traffic

See [[Application-Based Multipath Routing.](#)]

Flow-Based and Packet-Based Processing

- **Support for PowerMode (SRX4100, SRX4200, SRX4600, SRX5400 SPC3, SRX5600 SPC3, SRX5800 SPC3, and vSRX)**—Starting in Junos OS Release 21.3R1, we introduce PowerMode to improve UDP and TCP firewall throughput performance. PowerMode is enabled by default. To disable the feature, use the `power-mode-disable` statement at the `[edit security flow]` hierarchy level.

[See [PowerMode](#), and [power-mode-disable](#).]

Intrusion Detection and Prevention

- **Support IDP Packet-log capture for the logical systems and tenant systems (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.3R1, you can capture IDP security packet logs for logical systems and tenant systems. With packet capture enabled on your security device, you can also specify a number of post-attack or pre-attack packets to capture. After you've configured packet capture on your security device, then the device collects the captured information and stores it as a packet capture (**.pcap**) file at the logical systems and tenant systems levels.

[See [IDP Security Packet Capture](#).]

J-Web

- **Packet capture support for dynamic applications and security policies (SRX Series)**—In Junos OS Release 21.3R1, we've introduced the following improvements for packet capture:
 - Configure packet capture globally to capture all unknown traffic. Go to **Security Policies & Objects > Dynamic Applications > Global Settings**.
 - Configure packet capture for a security policy to capture unknown application traffic specific to a security policy rule. Go to **Security Policies & Objects > Security Policies > Advanced Services**.
 - View the packet capture statistics and log details, download **.pcap** files, or delete **.pcap** files. Go to **Monitor > Logs > Session**.

[See [Global Settings](#), [Add a Rule](#), and [Monitor Session](#).]

- **Flexible VLAN tagging and native VLAN ID support for link aggregation (SRX Series)**—In Junos OS Release 21.3R1, we support flexible VLAN tagging and native VLAN ID for link aggregation. Flexible VLAN tagging supports transmission of 802.1Q VLAN single-tag and dual-tag frames on logical interfaces on the same Ethernet port. We've also enhanced the Link Aggregation page for better experience:
 - Renamed the VLAN Tagging column as VLAN Tagging Type.
 - On the Add AE Interface page:

- Renamed General Settings as General.
- Renamed Advanced Settings as Link Aggregation Control Protocol (LACP).
- Added VLAN tagging types.

[See [About the Link Aggregation Page](#).]

- **Support to add devices to Juniper Security Director Cloud (SRX Series)**—In Junos OS Release 21.3R1, you can add your SRX Series device to Juniper Security Director Cloud. Use the **Add Device to Juniper Security Director Cloud** icon located at the top-right corner of the J-Web UI. After adding the device, you can manage your network security using Juniper Security Director Cloud.

NOTE: Before adding your device, ensure that:

- The device has Internet connectivity and access to the Juniper Security Director Cloud portal.
- The device's TCP and UDP ports are open so that it communicates with Juniper Security Director Cloud.

[See [Add an SRX Device to Juniper Security Director Cloud](#).]

- **Inclusion and diversity changes (SRX Series)**—In Junos OS Release 21.3R1, we've changed some of the terminologies used on the following pages. The changed terms represent the inclusion and diversity principles we value.
 - Security Services > UTM > Default Configuration
 - Security Services > UTM > Antivirus Profiles
 - Security Services > UTM > Antispam Profiles
 - Security Policies & Objects > Zones/Screens > Screen List
 - Network > Routing > RIP
 - Network > Routing > BGP

[See [Add a Screen](#), [About the Antivirus Profiles Page](#), and [About the Antispam Profiles Page](#).]

- **VPN Monitoring widget on the Dashboard page (SRX Series)**—In Junos OS Release 21.3R1, we've added a new VPN Monitoring widget on the Dashboard page. Use the VPN Monitoring widget to view the total number of IPsec VPNs (Total number of VPNs for All VPNs and total number of remote users for Remote Access).

[See [J-Web Dashboard](#).]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **Advanced Strike Engine (SRX Series)**—Starting in Junos OS Release 21.3R1, a new high performance malware inspection engine has been added to SRX Series devices. The device can block a malicious file immediately inline when an advanced anti-malware policy is configured with the block action. This enhancement to Juniper ATP Cloud block mode is supported on HTTP, IMAP and, SMB protocols.

NOTE: Starting in Junos OS Release 21.3R1, AAMW HTTP hash solution is deprecated.

Use the existing `set services advanced-anti-malware policy policy-name http action block` command to configure block mode. To view the malware statistics, use the `show services advanced-anti-malware malware-db-statistics operational` command.

[See [advanced-anti-malware policy](#) and [show services advanced-anti-malware statistics](#).]

Network Management and Monitoring

- **Support for on-box reporting (SRX300, SRX320, SRX340, SRX345, and SRX550HM)**—Starting in Junos OS Release 21.3R1, on-box reporting logs are stored on the memory file system (MFS) which is not persistent across reboots or power failures. For customers who wish to retain security logs between reboots, the dedicated log-storage SSD (JSU-SSD-MLC-100) must be installed in the device (SRX340 or SRX345).

[See [Understanding On-Box Logging and Reporting](#).]

- **SNMP support to view configured logical systems and tenant systems details (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 21.3R1, you can view the following details of configured logical systems and tenant systems using the new LSYSTSYS MIB:

- Total logical system count
- Total tenant system count
- Total security profiles count
- Maximally allowed logical system capacity
- Maximally allowed tenant system capacity
- Maximally allowed security profiles capacity

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

- **Support for syslog over TLS (SRX Series and vSRX)**—Starting in Junos OS Release 21.3R1, you can transport syslog (control plane) over Transport Layer Security (TLS) protocol. Encapsulating syslog in TLS allows you to:
 - Validate the remote destination (syslog server) before transmitting any sensitive syslog information. (Authentication)
 - Encrypt the syslog during the transport. (Encryption)
 - Verify that the data has not been modified or tampered with (Integrity)

Before you enable this feature, ensure you:

- Configure public key infrastructure (PKI) in Junos OS
- Configure and load the digital certificates
- Configure the remote destination (syslog server) that supports syslog over TLS

To enable transport of syslog (control plane) over TLS, use the `tls` statement at the `[edit system syslog host host-name transport]` hierarchy level.

[See [tlsdetails](#) and [transport](#)]

VPNs

- **Support for IPsec tunnel MTU (MX240, MX480, and MX960 with MX-SPC3, SRX5400, SRX5600, and SRX5800 with SPC3, and and vSRX devices)**— Starting in Junos OS Release 21.3R1, you can configure the MTU size for IPsec tunnels. This configuration defines the maximum size of an IP packet, including the IPsec overhead.

On IPv6, we provide support to disable the ICMPv6 Packet Too Big error message.

[See [Configuring IPsec VPN on MX-SPC3 Services Card](#).]

Additional Features

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

- **Juniper Secure Connect and NCP Exclusive Remote Access Client with ikev2 process** (SRX5000 line of devices with SPC3 and vSRX 3.0 running ikev2)

[See [Juniper Secure Connect](#) and [Remote Access VPNs with NCP Exclusive Remote Access Client](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.3R2 | 223](#)
- [What's Changed in Release 21.3R1 | 224](#)

Learn about what changed in this release for SRX Series.

What's Changed in Release 21.3R2

IN THIS SECTION

- [Authentication and Access Control | 223](#)
- [General Routing | 223](#)
- [J-Web | 224](#)
- [Network Management and Monitoring | 224](#)

Authentication and Access Control

- **Enhanced UAC authentication (SRX Series)**— To regulate the lifespan (default 60 seconds) of event table entries, we've added a new configuration statement `set services unified-access-control event-table-lifetime time interval in seconds` . If there is a delay in authentication at the SRX Series device, use this configuration statement to enable UAC traffic after the user is authorized from the IC.

[See [Configuring Junos OS Enforcer Failover Options \(CLI Procedure\)](#).]

General Routing

- **No support for PKI operational mode commands on the Junos Limited version (MX Series, PTX Series, and SRX Series devices)**— We do not support `request` , `show` , and `clear` PKI-related operational commands on the limited encryption Junos image ("Junos Limited"). If you try to execute PKI operational commands on a limited encryption Junos image, then an appropriate error message is displayed. The `pkid` process does not run on Junos Limited version image. Hence, the limited version does not support any PKI-related operation.

J-Web

- **Changes to the Dashboard and Monitor pages (SRX Series)**— To improve the J-Web UI loading speed: On the Dashboard page, we've removed the on-box reports related widgets. On the Monitor > Maps and Charts > Traffic Map page, we've changed the default duration from Last 1 hour" to Last "5 minutes."

Network Management and Monitoring

- Change in behavior of SNMP MIB object ifAlias---SNMP MIB object ifAlias now shows the configured interface alias. In earlier releases, ifAlias used to show configured interface description.
- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
 - When you deactivate the entire [edit system configuration-database ephemeral] hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
 - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
 - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the delete-ephemeral-default statement in conjunction with the ignore-ephemeral-default statement at the [edit system configuration-database ephemeral] hierarchy level.

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

What's Changed in Release 21.3R1

IN THIS SECTION

- [Junos XML API and Scripting | 225](#)
- [Network Management and Monitoring | 225](#)
- [VPNs | 225](#)

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS.](#)]

Network Management and Monitoring

- **Enhancement to the snmp mib walk command (PTX Series, QFX Series, EX Series, MX Series, SRX Series)**—The `ipv6IfOperStatus` field displays the current operational state of the interface. The `noIfIdentifier(3)` state indicates that no valid Interface Identifier is assigned to the interface. This state usually indicates that the link-local interface address failed Duplicate Address Detection. When you specify the 'Duplicate Address Detected' error flag on the interface, the new value (`noIfIdentifier(3)`) is displayed. Previously, the `snmp mib walk` command did not display the new value (`noIfIdentifier(3)`).
- **Changes in contextEngineID for SNMPv3 INFORMS (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Now the `contextEngineID` of SNMPv3 INFORMS is set to the local engine-id of Junos devices. In earlier releases, the `contextEngineID` of SNMPv3 INFORMS was set to remote engine-id.

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

VPNs

- **Deprecating Dynamic VPN CLI configuration statements and operational commands (SRX Series Devices)**—Starting in Junos OS Release 21.4R1, we'll be deprecating the dynamic VPN remote access solution. This means that you cannot use Pulse Secure Client on these devices.

As part of this change, we'll be deprecating the `[edit security dynamic-vpn]` hierarchy level and its configuration options. We'll also be deprecating the `show` and `clear` commands under the `[dynamic-vpn]` hierarchy level.

As an alternative, you can use the Juniper Secure Connect remote access VPN client that we introduced in Junos OS Release 20.3R1. Juniper Secure Connect is a user-friendly VPN client that supports more features and platforms than dynamic VPN does. SRX comes with two built-in concurrent users on all SRX Series devices. If you need additional concurrent users, then contact your Juniper Networks representative for remote-access licensing. To understand more about Juniper Secure Connect licenses, see [Licenses for Juniper Secure Connect and Managing Licenses](#).

[See [Juniper Secure Connect User Guide](#), [Juniper Secure Connect Administrator Guide](#), [Licenses for Juniper Secure Connect](#), and [Managing Licenses](#) .]

Known Limitations

IN THIS SECTION

- [Infrastructure](#) | 226
- [VPNs](#) | 226

Learn about known limitations in Junos OS Release 21.3R2 for SRX Series devices.

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

Infrastructure

- Use the no-validate option request system software add no-validate command when upgrading software from Junos OS release 21.1 or earlier to Junos OS release 21.2R1 or later. [PR1568757](#)

VPNs

- On SRX5400, SRX5600, and SRX5800 devices, during in-service software upgrade (ISSU), the IPsec tunnels flap, causing a disruption of traffic. The IPsec tunnels recover automatically after the ISSU process is completed. [PR1416334](#)
- 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

- [Authentication and Access Control | 227](#)
- [Flow-Based and Packet-Based Processing | 227](#)
- [General Routing | 228](#)
- [Interfaces and Chassis | 229](#)
- [Intrusion Detection and Prevention \(IDP\) | 229](#)
- [J-Web | 229](#)
- [Network Address Translation \(NAT\) | 229](#)
- [Platform and Infrastructure | 229](#)
- [VPNs | 230](#)

Learn about open issues in Junos OS Release 21.3R2 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.

Authentication and Access Control

- After a radius service is restored, SRX Series device do not send a RADIUS REQUEST message to that radius server, which causes authentication requests to time out. [PR1366002](#)

Flow-Based and Packet-Based Processing

- Use an antireplay window size of 512 for IPv4 or IPv6 in fat-tunnel. The ESP sequence check might otherwise report out-of-order packets if the fat-tunnel parallel encryption is within 384 packets (12 cores * 32 packets in one batch). Hence, there are no out-of-order packets with 512 antireplay window size. [PR1470637](#)

General Routing

- The rpd process might stop if a BGP route is resolved over the same prefix protocol next hop in the inet.3 table that has both RSVP and LDP routes.

[PR1458595](#)

- PKID core might occur during cert signature validation. This core is not very frequent and occurs due to memory corruption. [PR1573892](#)
- 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 AP mode on-box logging in Logical Systems and Tenant Systems, Intermittently Security log contents of binary log file in Logical Systems are not as expected. [PR1587360](#)
- Unexpected port value 0 is seen instead of undefined. [PR1589598](#)
- On SRX345 device, ICMP checksum error and packet drops are observed while doing rapid ping on vdsl interface with MTU 1514. [PR1591230](#)
- There is a behavior change in APPTRACK logs. By default logs are disabled. [PR1591966](#)
- In Junos OS releases 20.3 R3, 20.4R3 and 21.1R2, sometimes on reboot schedule-report are not getting generated. [PR1594377](#)
- Intermittently the trace messages are not logged on sending multicast traffic. [PR1598930](#)
- The switch reason is being shown as nh change instead of sla violated in the best path log message. [PR1602571](#)
- The AAMW Hash feature is deprecated. [PR1604426](#)
- The issue is when we enable TCP path finder in the VPN gateway, VPN connection is established properly. After VPN connection is established, able to ping from JSC installed CLIENT to SERVER behind gateway, but unable to ping from SERVER behind gateway to JSC installed CLIENT. [PR1611003](#)
- The t1 interface admin status will be shown as test instead of down during FPC failover. [PR1615494](#)
- On SRX1500, SRX380, SRX300, SRX320, SRX340, SRX345, SRX4200, SRX4600, SRX550, NFX150, and NFX250 Series devices with AppQoE configured, in a race condition that a short live data session is destroyed but passive probing is happening for that session concurrently, this condition might cause the flowd process to stop. [PR1621495](#)
- FIPS mode enabling fails with self-test failure and kernel stop. [PR1623128](#)

Interfaces and Chassis

- Traffic drop might be seen on irb interface on SRX1500 devices for network control forwarding class when verifying dscp classification based on single and multiple code-points. [PR1611623](#)

Intrusion Detection and Prevention (IDP)

- While executing CLI show security idp attack attack-list policy combine-policy, CLI might get stuck and only partial output gets displayed. CLI recovers in its own. This issues is seen very rarely. [PR1616782](#)

J-Web

- Adding a new VPN in CLI with J-Web logged in and user in dashboard page. To reflect the changes in dashboard, if out of band configuration changes (changes done in CLI), on refresh of dashboard widget changes will not be reflected until cache re-syncs. You have to navigate to some other menu or log out and log in and come back where the cache sync will happen and latest data will be displayed. [PR1589868](#)
- For Dynamic VPN configuration, topology is shown as 'Site to Site / Hub and Spoke' under Monitor - > Network -> IPsec VPN page. [PR1597889](#)
- When ADVPN or Auto Connect VPN has more than one IPsec VPN connections, J-Web displays any one of the remote gateway's IP address as Remote IP in the VPN Monitoring widget. [PR1599027](#)

Network Address Translation (NAT)

- In AA mode with NAT configuration, on RG failover, traffic getting dropped on SRX Series devices. [PR1636596](#)

Platform and Infrastructure

- The commit synchronize command fails because the kernel socket gets stuck. [PR1027898](#)

- On SRX Series devices with BFD enabled for multiple protocols (such as OSPF, ISIS, BGP, PIM), the ppmmd process might stop after an upgrade. [PR1335526](#)
- On SRX Series devices, if the SNMP packet (traps or polls) has to cross multiple routing-instances, it will cause the packet to be dropped due to incorrect routing-instance ID added by SRX. [PR1616775](#)

VPNs

- In some scenarios, sometimes SRX5000 line of devices might show obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. [PR1432925](#)
- An IPsec policy must not have both ESP and AH proposals. The configuration will commit, but the IPsec traffic will not work. Do not configure an IPsec policy with proposals using both ESP and AH protocols. [PR1552701](#)
- Fragment packets through policy-based IPsec tunnel could be dropped in some rare case when PMI is enabled. [PR1624877](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 231](#)
- [Resolved Issues: 21.3R1 | 234](#)

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

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

Resolved Issues: 21.3R2

IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 231](#)
- [Flow-Based and Packet-Based Processing | 231](#)
- [General Routing | 231](#)
- [Interfaces and Chassis | 233](#)
- [Intrusion Detection and Prevention \(IDP\) | 233](#)
- [J-Web | 233](#)
- [Platform and Infrastructure | 234](#)
- [Routing Policy and Firewall Filters | 234](#)
- [Routing Protocols | 234](#)
- [VPNs | 234](#)

Application Layer Gateways (ALGs)

- Junos OS: MX Series and SRX Series: The flowd daemon will crash if the SIP ALG is enabled and specific SIP messages are processed (CVE-2022-22175). [PR1604123](#)

Flow-Based and Packet-Based Processing

- The Services-offload packets processed counter not incremented in security flow statistics. [PR1616875](#)
- Security traffic log display service-name=None for some application. [PR1619321](#)
- Cleartext fragments are not processed by flow. [PR1620803](#)
- VLAN tagged packets might be dropped at TAP mode enabled interface. [PR1624041](#)

General Routing

- Some transmitting packets might get dropped due to the disable-pfe action is not invoked when the fabric self-ping failure is detected. [PR1558899](#)
- When using log templates introduced in Junos OS release 21.1R1 with Unified Policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a

default log profile set security log profile name default-profile command can be used to improve this behavior when multiple log profiles are defined. [PR1570105](#)

- The fxp0 interface of an SRX550 device in cluster might become unreachable from an external network. [PR1575231](#)
- HTTP sessions are not re-established fine after a link flap between hub and spoke. [PR1577021](#)
- The error message tcp_timer_keep:Local(0x81100001:60753) Foreign(0x8f100001:33010) is seen in messages log every 80 seconds. [PR1580667](#)
- Getting UNKNOWN instead of HTTP-PROXY for application and UNKNOWN instead of GOOGLE-GEN in RT-FLOW close messages. [PR1588139](#)
- When combining log profiles and unified policies RT_FLOW_SESSION_DENY logs were not being generated corrected. [PR1594587](#)
- Traffic might be dropped at NAT gateway if EIM is enabled. [PR1601890](#)
- Kernel pause might be seen when static routes are configured with GRE interfaces being used as next-hop. [PR1601996](#)
- When the tap mode is enabled, the packet on ge-0/0/0 is dropped on RX side. [PR1606293](#)
- DNS proxy functionality might not work on VRRP interfaces. [PR1607867](#)
- Enabling security-metadata-streaming-policy might cause Packet Forwarding Engine stop. [PR1610260](#)
- DNS-based SecIntel statistics were not populating correctly on SRX Series devices. [PR1611071](#)
- On SRX Series devices running DNS Security, the notification option log-detections was not honoured. Prior to this release, a log was generated for every DNS request, regardless of its intent (malicious or benign). [PR1611177](#)
- Interface might not come up when 10G port is connected to 1G SFP. [PR1613475](#)
- Enabling security-metadata-streaming DNS policy might cause a dataplane memory leak. [PR1613489](#)
- On SRX Series devices running DNS Security in secure-wire mode, DGA verdicts would not be returned to the device. [PR1616075](#)
- The srxpfe process might stop when the DNS Security feature is enabled. [PR1616171](#)
- On SRX Series devices using on-box logging, LLMD write failures might be seen under high load. The output of show security log llmd counters command can be used to view LLMD behavior. [PR1620018](#)
- Traffic might get dropped due to memory issue on some SRX Series devices. [PR1620888](#)

- Under rare circumstances, an srxpfe or flowd process generates core files when running advanced-anti-malware. [PR1624124](#)
- Running DNS on all SRX Series devices, a memory leak on Packet Forwarding Engine might occur. [PR1624655](#)
- Core files might be reported on installing IDP security package. [PR1625364](#)
- The flowd process lost heartbeat for 45 consecutive seconds without alarm raised. [PR1625579](#)
- When viewing DNS Tunnel detections in the ATP Cloud portal, the Source-IP and Destination-IP metadata is reversed. [PR1629995](#)
- Depending on the configuration of the SRX Series devices, duplicate events might have been written to the on-box logging database. This fix improves LLMD performance by eliminating these duplicate write events. [PR1630123](#)
- LLDP packets might be sent with incorrect source MAC for RETH or LAG child members. [PR1630886](#)
- Reverse DNS Lookups will no longer be stored in the DNSF Cache when using DNS Security. [PR1631000](#)

Interfaces and Chassis

- IPv4 or IPv6 address might get removed when the interface configuration is moved from tenant stanza to interface stanza. [PR1605250](#)

Intrusion Detection and Prevention (IDP)

- High Routing Engine CPU usage occurs when routing-instance is configured under security idp security-package hierarchy level. [PR1614013](#)
- IDP signature install taking longer time. [PR1615985](#)
- ApplD database update failing to download when used through IDP offline method. [PR1623857](#)

J-Web

- Your session has expired. Click ok to re-login when using root user. [PR1611448](#)
- The AM or PM time format is displayed in customize for last field at Monitor > Logs > All Events. [PR1628649](#)

Platform and Infrastructure

- SRX Accounting and auditd process might not work on secondary node. [PR1620564](#)
- Error message "gencfg_cfg_msg_gen_handler drop" is seen after running commit command. [PR1629647](#)

Routing Policy and Firewall Filters

- High CPU usage might be seen on some SRX Series devices. [PR1579425](#)

Routing Protocols

- Observing commit error while configuring routing-options rib inet6.0 static on all Junos OS devices. [PR1599273](#)

VPNs

- The iked process might restart and generate core during session state activation or deactivation. [PR1573102](#)
- Certificate identifier length for PKI CMPv2 CA cert is not displayed as expected in certain cases. [PR1589084](#)
- Tail drops might occur on SRX Series devices if shaping-rate is configured on st-interface. [PR1604039](#)
- Authentication might fail on bringing up IPsec tunnel when ECDSA is configured in the security ike. [PR1605275](#)
- Traffic over IPSec tunnels might be dropped post control link failure. [PR1627557](#)

Resolved Issues: 21.3R1

IN THIS SECTION

- [Authentication and Access Control | 235](#)
- [Chassis Clustering | 235](#)
- [Flow-Based and Packet-Based Processing | 235](#)
- [Uncategorized | 235](#)
- [Infrastructure | 238](#)

- Interfaces and Chassis | [238](#)
- Intrusion Detection and Prevention (IDP) | [238](#)
- J-Web | [238](#)
- Network Address Translation (NAT) | [239](#)
- Platform and Infrastructure | [239](#)
- Routing Policy and Firewall Filters | [239](#)
- Routing Protocols | [239](#)
- Services Applications | [239](#)
- Unified Threat Management (UTM) | [240](#)
- User Interface and Configuration | [240](#)
- VPNs | [240](#)

Authentication and Access Control

- Unified-access-control (UAC) authentication might not work post system reboot. [PR1585158](#)

Chassis Clustering

- Security policies might not be synced to all Packet Forwarding Engines post upgrade. [PR1591559](#)

Flow-Based and Packet-Based Processing

- The srpxfe process might crash during route churn. [PR1572240](#)
- On SRX Series devices, the filter from-zone has been added to the utility monitor security packet-drop. [PR1574060](#)
- Performance degradation might be observed when power-mode-ipsec is enabled. [PR1599044](#)

Uncategorized

- SSL-FP logging for non SNI session. [PR1442391](#)
- The flowd might core dump frequently on SRX340 device. [PR1463689](#)
- PKI CMPv2 client certificate enrollment does not work on SRX when using root-CA. [PR1549954](#)

- Application identity unknown packet capture utility does not function on SRX Series devices when enhanced-services mode is enabled. [PR1558812](#)
- Some transmitting packets might get dropped due to the disable-pfe action is not invoked when the fabric self-ping failure is detected. [PR1558899](#)
- The PIC in SRX5K-SPC3 and MX-SPC3 card might get stuck in offline status after flowd crash occurs on it. [PR1560305](#)
- The show pfe statistics traffic command shows wrong output. [PR1566065](#)
- Packets with the MAC address of eth0 and macvlan0@eth0 interface might be sent out to the management interface on VMHOST platform with NG-RE. [PR1571753](#)
- Traffic is dropped to or through VRRP virtual IP on SRX380 device. [PR1581554](#)
- The ipfd process might crash with a core dump when SecProfiling thread feeds are fetched from Policy Enforcer(PE). [PR1582454](#)
- The srxpfe process might crash on SRX1500 device. [PR1582989](#)
- Packet drop or srxpfe core dump might be observed due to Glacis FPGA limitation. [PR1583127](#)
- The APPID process might crash with a core if multiple commands are run simultaneously. [PR1583606](#)
- Secure Web proxy continue sending DNS query for unresolved DNS entry even after the entry was removed. [PR1585542](#)
- On SRX Series devices, significant performance improvements for JDPI's micro-application identification were included in this release. [PR1585683](#)
- The 1G interfaces might not come up after device reboot. [PR1585698](#)
- The l2ald process might crash on issuing ethernet-switching commands. [PR1586426](#)
- The l2ald process might crash on changing the routing-instance. [PR1586516](#)
- On SRX Series devices, the protocol-version command which controls TLS-versions (1.1, 1.2, 1.3, etc) within SSL-Proxy has been unhidden. [PR1587149](#)
- On SRX Series devices, the unknown packet-capture functionality will no longer record SSL. UNKNOWN flows by default. This behavior can be changed by enabling the set services application-identification packet-capture ssl-unknown command. Without configuration the ssl-unknown command, the SRX will only capture flows marked as UNKNOWN or INCONCLUSIVE. [PR1587875](#)
- Garbage characters might be received in quarantine notification. [PR1587962](#)
- IP packets might be dropped on SRX Series devices. [PR1588627](#)

- The jsqsyncd process files generation might cause device to panic crash after upgrade. [PR1589108](#)
- SRX connection to Juniper Secure Connect might fail with IKE negotiation request from user disallowed as remote-access user license limit exceeded. [PR1589865](#)
- Pass-through traffic might fail post reboot when Secure Web Proxy is configured. [PR1589957](#)
- Traffic loss might be observed for interface configured in subnet 137.63.0.0/16. [PR1590040](#)
- The REST API does not work for SRX380 device. [PR1590810](#)
- The issue (empty feed-name) starts with the hit returned from cache which points to the node with the parameter of feed-ID (2) inconsistent with the feeds-update (when it's 1). As a result the incorrect feed-ID points to the empty entry in the array of the feed-names. [PR1591236](#)
- J-Web deny log nested-application="UNKNOWN" instead of specific application. [PR1593560](#)
- System log will be generated when max-session or total memory limit is hit for packet capture. [PR1594669](#)
- Node1 fpc0 (SPM) goes down after ISSU and RGO failover. [PR1595462](#)
- Network based application recognition value for IPv4 application-id are not as expected. [PR1595787](#)
- Delay might be observed between Services Processing Card (SPC) failing and failover to other node. [PR1596118](#)
- The flowd process might generate core files if the application-services security policy is configured. [PR1597111](#)
- The srxpfe process might stop and generate a core file post targeted-broadcast forward-only command interface configuration commit. [PR1597863](#)
- The flowd process might generate core files if the AppQOS module receiving two packets of a session. [PR1597875](#)
- The flowd process might stop in AppQoS scenarios. [PR1599191](#)
- The httpd-gk core file might be observed when IPsec VPN is configured. [PR1599398](#)
- The flowd process might crash if the DNS inspection feature is enabled by configuring SMS policy. [PR1604773](#)
- Memory leak at the useridd process might be observed when Integrated User Firewall is configured. [PR1605933](#)
- When the tap mode is enabled, the packet on ge-0/0/0 is dropped on RX side. [PR1606293](#)
- The flowd process might stop if the DNS inspection feature is enabled within SMS. [PR1607251](#)

- Enabling dnsf traceoptions on SRX300 lines of devices might result in flowd crash. [PR1608669](#)
- Enabling security-metadata-streaming-policy might cause Packet Forwarding Engine pause. [PR1610260](#)
- On the SRX4600, when you connect a 1G SFP to the 10G port, a reboot is required. A new critical log will now be introduced so the requirement is more visible. In chassis clusters of SRX4600, both nodes need to be rebooted at the same time. [PR1613475](#)

Infrastructure

- VM might crash if file is shared between host operating system and guest operating system using virtFS. [PR1551193](#)

Interfaces and Chassis

- Facing configuration check-out failed with error message, the identical local address found on rt_inst [default] and intfs. [PR1581877](#)
- The IPv4 or IPv6 address from the configuration on the interface might not be applied when the interface is moved from tenants to interface stanza in the configuration. [PR1605250](#)

Intrusion Detection and Prevention (IDP)

- Adding signature in packet drop reason and sending to record packet drops module. [PR1574603](#)
- IDP policy compilation failure for over 1000 custom signatures. [PR1589399](#)
- IDP signature DB update fails. [PR1594283](#)
- Custom attack IDP policies might fail to compile. [PR1598867](#)
- IDP policy compilation is not happening when a commit check is issued prior to a commit. [PR1599954](#)
- The srxpfe might stop while the IDP security package contains a new detector. [PR1601380](#)
- This release includes optimizations made to IDP that help improve its performance and behavior under load. [PR1601926](#)

J-Web

- Junos OS: J-Web allows a locally authenticated attacker to escalate their privileges to root. (CVE-2021-0278) [PR1511853](#)

- The zone info disappears when functional zone is configured. [PR1594366](#)
- A custom application name contains "any" is listed under predefined applications. [PR1597221](#)
- J-Web might not display customer defined application services if one new policy is created. [PR1599434](#)
- J-Web application might stop and generates httpd core files. [PR1602228](#)
- Radius users might not be able to view or modify configuration through J-Web. [PR1603993](#)
- On all SRX Series devices, some widgets in J-Web might not load properly for logical systems users. [PR1604929](#)

Network Address Translation (NAT)

- Incorrect IPv6 UDP checksum inserted after translation of packet from IPv4 to IPv6 addresses. [PR1596952](#)

Platform and Infrastructure

- Junos OS: Upon receipt of specific sequences of genuine packets destined to the device the kernel will crash and restart (vmcore) (CVE-2021-0283, CVE-2021-0284). [PR1557881](#)

Routing Policy and Firewall Filters

- The dns-name cannot be resolved if customer-defined routing instance is configured under name-server. [PR1539980](#)

Routing Protocols

- Short multicast packets drop using PIM when multicast traffic received at a non-RPT or SPT interface [PR1579452](#)
- BGP session carrying VPNv4 prefix with IPv6 next-hop might be dropped. [PR1580578](#)
- The fwauthd process generates core files when upgrading to Junos OS release 21.2R1. [PR1588393](#)

Services Applications

- Extra data plane CPU cycles for processing GTP traffic on SRX5000 line of devices. [PR1586367](#)

Unified Threat Management (UTM)

- There is no counter for juniper-local default action. [PR1570500](#)

User Interface and Configuration

- During rare circumstances, the mgd process might stop and generate a core file on Junos devices connected with Contrail Service Orchestration (CSO). [PR1569903](#)
- The juniper.conf.gz file creates with empty data when we create an tenant system. [PR1584850](#)
- After image upgrade device might fail to come up due to certain configurations. [PR1585479](#)
- IS-SU upgrade aborted from Junos OS release 21.1R1.11 to Junos OS release 21.2I-20210415.0.0138 on SRX5000 lines of devices with chassis cluster. [PR1590099](#)

VPNs

- The pkid core dumping while auto-enrollment of local certificates. [PR1564300](#)
- The srxpfe process might stop and generate a core file when IPsec VPN is used. [PR1574409](#)
- IKEv2 soft-lifetime timer might expire later than expected time. [PR1574717](#)
- The iked process might crash when IKEv2 negotiation fails on MX and SRX Series devices. [PR1577484](#)
- The from-self packet might be dropped when it forwards through an IPsec VPN tunnel. [PR1577550](#)
- The ikemd process might crash when SNMP get is performed on jnxIpSecTunnelMonTable. [PR1582036](#)
- Memory leaks on the iked process on SRX5000 line of devices with SRX5K-SPC3 installed. [PR1586324](#)
- The IPSec tunnel might not come up if configured with configuration payload in a certain scenario. [PR1593408](#)
- The kmd process might crash when VPN peer initiates using source-port other than 500. [PR1596103](#)
- Tail drops might occur on SRX Series devices if shaping-rate is configured on st-interface. [PR1604039](#)
- Authentication fails on bringing up IPsec tunnel between DUT and Strongswan-peer with IKE (group21 sha-512 aes-192-cbc) proposal. [PR1605275](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R2 documentation for SRX Series devices.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 241

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 8: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the [Installation and Upgrade Guide](#).

Junos OS Release Notes for vMX

IN THIS SECTION

- [What's New | 243](#)
- [What's Changed | 243](#)
- [Known Limitations | 245](#)
- [Open Issues | 245](#)
- [Resolved Issues | 245](#)
- [Documentation Updates | 247](#)
- [Upgrade Instructions | 247](#)

These release notes accompany Junos OS Release 21.3R2 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

- [What's New | 243](#)

Learn about new features introduced in this release for vMX.

What's New

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

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.3R2 | 244](#)
- [What's Changed in Release 21.3R1 | 244](#)

Learn about what changed in this release for vMX.

What's Changed in Release 21.3R2

IN THIS SECTION

- [Network Management and Monitoring | 244](#)

Network Management and Monitoring

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
 - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
 - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
 - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

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

What's Changed in Release 21.3R1

IN THIS SECTION

- [Junos XML API and Scripting | 244](#)

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a

hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS](#).]

Known Limitations

There are no known limitations in hardware and software in Junos OS 21.3R2 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 and software in Junos OS 21.3R2 for vMX.

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

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 246](#)
- [Resolved Issues: 21.3R1 | 246](#)

Learn about the issues fixed in this release for vMX.

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

Resolved Issues: 21.3R2

IN THIS SECTION

- [Platform and Infrastructure | 246](#)

Platform and Infrastructure

- CFM enhanced SLA iterators monitoring might stop after restarting chassis-control process in vMX. [PR1622081](#)

Resolved Issues: 21.3R1

IN THIS SECTION

- [Forwarding and Sampling | 246](#)
- [General Routing | 246](#)

Forwarding and Sampling

- The l2ald process might crash when you change the routing-instance. [PR1584737](#)
- IS-IS LSP might not be originated if egress protection is configured. [PR1605969](#)
- The rpd core might be seen on all Junos OS and Junos OS Evolved platforms. [PR1613384](#)

General Routing

- The MX150 device might reboot after you issue the `request system snapshot recovery` command. [PR1565138](#)
- On MX150 routers, the interface might take a long time to power down while rebooting, powering-off, halting, or upgrading. [PR1575328](#)
- Communication between two CE devices might fail when you enable the BGP rib-sharding. [PR1582210](#)

- The bcmd process might crash on the MX150 platform. [PR1583281](#)
- Interface hold-time up does not work on vMX and MX150 platforms. [PR1604554](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R2 documentation 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

- [What's New | 248](#)
- [What's Changed | 249](#)
- [Known Limitations | 249](#)
- [Open Issues | 249](#)
- [Resolved Issues | 250](#)
- [Documentation Updates | 250](#)

These release notes accompany Junos OS Release 21.3R2 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

- [What's New in 21.3R2 | 248](#)
- [What's New in 21.3R1 | 248](#)

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

There are no new features for vRR in Junos OS Release 21.3R2.

What's New in 21.3R2

There are no new features or enhancements to existing features for vRR in Junos OS Release 21.3R2.

What's New in 21.3R1

IN THIS SECTION

- [Application Identification \(AppID\) | 248](#)

There are no new features or enhancements to existing features for vRR in Junos OS Release 21.3R1.

Application Identification (AppID)

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.3R2 | 249](#)

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

To learn more about common BGP or routing changes in behavior or syntax in Junos OS 21.3R1, see ["What's Changed" on page 78](#) for MX Series routers.

What's Changed in Release 21.3R2

There are no changes in behavior and syntax in Junos OS Release 21.3R2 for vRR.

Known Limitations

There are no known limitations in hardware and software in Junos OS 21.3R2 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 21.3R2, see ["Known Limitations" on page 83](#) for MX Series routers.

Open Issues

There are no known issues in hardware and software in Junos OS Release 21.3R2 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 issues in Junos OS 21.3R2, see ["Open Issues" on page 85](#) for MX Series routers.

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 250](#)

There are no resolved issues 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 resolved issues in Junos OS 21.3R1, see "[Resolved Issues](#)" on [page 96](#) for MX Series routers.

Resolved Issues: 21.3R2

IN THIS SECTION

- [General Routing | 250](#)

General Routing

- Memory might be exhausted when both the BGP rib-sharding and the BGP ORR is enabled. [PR1613104](#)
- The rpd process might stop in BGP rib-sharding scenario. [PR1613723](#)
- The monitor traffic interface does not work on em2. [PR1629242](#)
- vRR VM might establish its identity as Olive after a CLI software upgrade. [PR1635950](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R2 documentation for vRR.

Junos OS Release Notes for vSRX

IN THIS SECTION

- [What's New | 251](#)
- [What's Changed | 252](#)
- [Known Limitations | 254](#)
- [Open Issues | 254](#)
- [Resolved Issues | 256](#)
- [Documentation Updates | 260](#)
- [Migration, Upgrade, and Downgrade Instructions | 260](#)

These release notes accompany Junos OS Release 21.3R1 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

- [What's New in 21.3R2 | 251](#)
- [What's New in 21.3R2 | 252](#)

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

What's New in 21.3R2

Learn about new features or enhancements to existing features in this release for the vSRX.

What's New in 21.3R2

Learn about new features or enhancements to existing features in this release for the vSRX.

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.3R2 | 252](#)
- [What's Changed in Release 21.3R1 | 253](#)

Learn about what changed in this release for vSRX.

What's Changed in Release 21.3R2

IN THIS SECTION

- [Network Management and Monitoring | 252](#)
- [VPNs | 253](#)

Network Management and Monitoring

- **Change in behavior of SNMP MIB object ifAlias**—SNMP MIB object ifAlias now shows the configured interface alias. In earlier releases, ifAlias used to show configured interface description.
- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
 - When you deactivate the entire [edit system configuration-database ephemeral] hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

- When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

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

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.

What's Changed in Release 21.3R1

IN THIS SECTION

- [Junos XML API and Scripting | 253](#)
- [Licensing | 253](#)

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS](#).]

Licensing

- **vCPU core based license and license key format (vSRX 3.0)** —When you are upgrading from Junos OS release 20.4R1 or earlier releases to Junos OS release 21.1R1 or later releases, you need new license

keys to use the features on the listed devices. Contact [Customer Care](#) to exchange license keys. For more information, see [vSRX 3.0 requires a vCPU core based license from Junos OS release 21.1R1 onwards](#).

Known Limitations

There are no known limitations in hardware and software in Junos OS 21.3R2 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

- [Flow-Based and Packet-Based Processing](#) | 254
- [General Routing](#) | 255
- [Intrusion Detection and Prevention \(IDP\)](#) | 255
- [J-Web](#) | 255
- [Network Address Translation \(NAT\)](#) | 256
- [VPNs](#) | 256

Learn about open issues in Junos OS Release 21.3R2 for vSRX.

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

Flow-Based and Packet-Based Processing

- Traffic in the power-mode still passthrough when the ingress logic interface is manually disabled. [PR1604144](#)

General Routing

- The tag `RT_FLOW_SESSION_XXX` is missing in stream mode. [PR1565153](#)
- Under very rare conditions for HA cluster deployment, when it does RGO failover and at same time, the control link is down, then it generates mib2d core files because the master Routing Engine and secondary Routing Engine are out of syncing dcd.snmp_ix information. [PR1571677](#)
- During auto-reenrollment of cmpv2 certificates, if the CA server is unresponsive and cmpv2 request retries has reached the maximum limit, then pkid might generate core file. [PR1580442](#)
- With ssl-proxy configured along with web-proxy, the client session might not closed on the device even though proxy session ends gracefully. [PR1580526](#)
- You can improve the vSRX performance using `set security forwarding-options no-allow-dataplane-sleep` command. [PR1602564](#)
- The switch reason is being shown as nh change instead of SLA violated in the best path log message. [PR1602571](#)
- Configure `set security forwarding-options no-allow-dataplane-sleep` command for high traffic rate use cases. [PR1602606](#)
- The AAMW Hash feature is deprecated. [PR1604426](#)

Intrusion Detection and Prevention (IDP)

- The `show security idp attack attack-list policy combine-policy` command might get stuck and only partial output gets displayed. The CLI recovers in its own. This issues is seen very rarely. [PR1616782](#)

J-Web

- Adding a new VPN in CLI with J-Web logged in and user in dashboard page. To reflect the changes in dashboard, if out of band configuration changes (changes done in CLI), on refresh of dashboard widget changes will not be reflected until cache re-syncs. You have to navigate to some other menu or log out and log in and come back where the cache sync will happen and latest data will be displayed. [PR1589868](#)
- When ADVPN or Auto Connect VPN has more than one IPsec VPN connections, J-Web displays any one of the remote gateway's IP address as Remote IP in the VPN Monitoring widget. [PR1599027](#)

Network Address Translation (NAT)

- The ICMPv6 TCP sequence information is missing in the ICMP v6 error generated. [PR1611202](#)

VPNs

- In certain cases, the PUSH ACK message from the group member to the group key server might be lost. The group member can still send rekey requests for the TEK SAs before the hard lifetime expiry. Only if the key server sends any new PUSH messages to the group members, those updates would not be received by the group member since the key server would have removed the member from registered members list. [PR1608290](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.3R2 | 256](#)
- [Resolved Issues: 21.3R1 | 258](#)

Learn about the issues fixed in this release for vSRX.

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

Resolved Issues: 21.3R2

IN THIS SECTION

- [General Routing | 257](#)
- [Intrusion Detection and Prevention \(IDP\) | 257](#)
- [Network Address Translation \(NAT\) | 258](#)

- [Routing Protocols | 258](#)
- [User Interface and Configuration | 258](#)
- [VPNs | 258](#)

General Routing

- When using log templates introduced in Junos OS release 21.1R1 with Unified Policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile set security log profile name default-profile command can be used to improve this behavior when multiple log profiles are defined. [PR1570105](#)
- Getting UNKNOWN instead of HTTP-PROXY for application and UNKNOWN instead of GOOGLE-GEN in RT-FLOW close messages These messages can be seen in the RT-flow close log and these are due to JDPI not engaged for the session. This might affect the application identification for the web-proxy session traffic. [PR1588139](#)
- When combining log profiles and unified policies RT_FLOW_SESSION_DENY logs were not being generated corrected. [PR1594587](#)
- vSRX might stop forwarding traffic 60 days after Junos OS upgrade due to the trial license expiring. [PR1609551](#)
- For apps getting classified on first packet, the volume update syslog is not getting generated. [PR1613516](#)
- The interface speed is limited to 1G on vSRX 2.0 even the speed is set as more than 1G. [PR1617397](#)
- Assert core might be seen when the application goes to no path selected state. [PR1617506](#)
- Running DNS on all SRX Series devices, a memory leak on Packet Forwarding Engine might occur. [PR1624655](#)
- Application package installation failed in Packet Forwarding Engine with error is seen while repetitive enabling or disabling of application or groups. [PR1626589](#)
- vSRX3 on VMware ESXi versions 7.0u2 or 7.0u3 with i40e SR-IOV, the traffic stopped after reboot. [PR1627481](#)

Intrusion Detection and Prevention (IDP)

- The flowd or srpxfe process might crash when IDP is used on Junos OS Release 21.2R1. [PR1610706](#)

Network Address Translation (NAT)

- The SNMP object jnxJsNatSrcNumPortAvail does not show the proper value. [PR1611479](#)

Routing Protocols

- The rpd might generate core files due to memory corruption. [PR1599751](#)

User Interface and Configuration

- A low privileged user can elevate their privileges to the ones of the highest privileged J-Web user logged in. [PR1593200](#)

VPNs

- Unable to set DynamoDB in HSM module. [PR1599069](#)

Resolved Issues: 21.3R1

IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 258](#)
- [Authentication and Access Control | 258](#)
- [Flow-Based and Packet-Based Processing | 259](#)
- [General Routing | 259](#)
- [Intrusion Detection and Prevention \(IDP\) | 259](#)
- [Platform and Infrastructure | 259](#)
- [VPNs | 260](#)

Application Layer Gateways (ALGs)

- ALG traffic might be dropped. [PR1598017](#)

Authentication and Access Control

- Unified-access-control (UAC) authentication might not work post system reboot. [PR1585158](#)

Flow-Based and Packet-Based Processing

- The srxpfe process might crash during route churn. [PR1572240](#)
- Multicast traffic drop might occur on TAP interface on SRX Series devices. [PR1583214](#)

General Routing

- IKE configure mode payload is not pushing secondary DNS and secondary WINS attributes to Xauth module with IKEv1. Hence, the client is not getting assigned with secondary DNS and secondary WINS with IKEv1. [PR1558831](#)
- The srxpfe or flowd process might crash when ATP is used. [PR1573157](#)
- The srxpfe process might stop and generate a core file during the feed update process. [PR1579631](#)
- Communication between two CEs might be failed when BGP rib-sharding is enabled. [PR1582210](#)
- The incorrect DNS UDP checksums might be generated when vSRX3.0 performs DNS Sinkhole. [PR1582827](#)
- vSRX unreachable over SSH after integration with KMS on AWS. [PR1584415](#)
- SRX connection to Juniper Secure Connect might fail with IKE negotiation request from user disallowed as remote-access user license limit exceeded. [PR1589865](#)
- Network based application recognition value for IPv4 application-id are not as expected. [PR1595787](#)
- The FPC might not come up if the vCPU number is configured more than 5 vCPU on vSRX3.0 platforms. [PR1601823](#)
- vSRX3 with Mellanox SR-IOV interfaces on VMware, the interface order is random. [PR1604060](#)
- vSRX might stop forwarding traffic 60 days after Junos OS upgrade due to the trial license expiring. [PR1609551](#)

Intrusion Detection and Prevention (IDP)

- APPID related signatures might not get triggered. [PR1588450](#)
- The flowd or srxpfe process might crash when IDP is used on Junos OS Release 21.2R1. [PR1610706](#)

Platform and Infrastructure

- COS queue egress interface forwarding-class might not work as expected. [PR1538286](#)

VPNs

- Unable to set DynamoDB in HSM module. [PR1599069](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.3R2 documentation for vSRX.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 266

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 21.3R2 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 21.3R2 for vSRX .tgz** file from the [Juniper Networks website](#). Note the size of the software image.
2. Verify that you have enough free disk space on the vSRX instance to upload the new software image.

```
root@vsrx> show system storage
```

Filesystem	Size	Used	Avail	Capacity	Mounted on
/dev/vtbd0s1a	694M	433M	206M	68%	/
devfs	1.0K	1.0K	0B	100%	/dev
/dev/md0	1.3G	1.3G	0B	100%	/junos
/cf	694M	433M	206M	68%	/junos/cf

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

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

```

root@vsrx> request system storage cleanup
List of files to delete:
Size Date      Name
11B Sep 25 14:15 /var/jail/tmp/alarmd.ts
259.7K Sep 25 14:11 /var/log/hostlogs/vjunos0.log.1.gz
494B Sep 25 14:15 /var/log/interactive-commands.0.gz
20.4K Sep 25 14:15 /var/log/messages.0.gz
27B Sep 25 14:15 /var/log/wtmp.0.gz
27B Sep 25 14:14 /var/log/wtmp.1.gz
3027B Sep 25 14:13 /var/tmp/BSD.var.dist
0B Sep 25 14:14 /var/tmp/LOCK_FILE
666B Sep 25 14:14 /var/tmp/appidd_trace_debug
0B Sep 25 14:14 /var/tmp/eedebg_bin_file
34B Sep 25 14:14 /var/tmp/gksdchk.log
46B Sep 25 14:14 /var/tmp/kmdchk.log
57B Sep 25 14:14 /var/tmp/krt_rpf_filter.txt
42B Sep 25 14:13 /var/tmp/pfe_debug_commands
0B Sep 25 14:14 /var/tmp/pkg_cleanup.log.err
30B Sep 25 14:14 /var/tmp/policy_status
0B Sep 25 14:14 /var/tmp/rtsdb/if-rtsdb
Delete these files ? [yes,no] (no) yes

```

```
<
output omitted>
```

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

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 21.3R2 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-x86-64-21.3-2022-01-01.0_RELEASE_21.3_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-
x86-64-21.3-2022-01-01.0_RELEASE_21.3_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-21.3-2022-01-01.0_RELEASE_21.3_THROTTLE signed by
PackageDevelopmentEc_2021 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING: This package will load JUNOS 21.3 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-21.3-2022-01-01.0_RELEASE_21.3_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-21.3-2022-01-01.0_RELEASE_21.3_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-21.3-2022-01-01.0_RELEASE_21.3_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-21.3-2022-01-01.0_RELEASE_21.3_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-21.3-2022-01-01.0_RELEASE_21.3_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-21.3-2022-01-01.0_RELEASE_21.3_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-21.3-2022-01-01.0_RELEASE_21.3_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-21.3-2022-01-01.0_RELEASE_21.3_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 21.3R2 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 21.3-2022-01-01.0_RELEASE_21.3_THROTTLE Kernel 64-bit
JNPR-11.0-20211012.170745_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: 21.3-2022-01-01.0_RELEASE_21.3_THROTTLE
JUNOS OS Kernel 64-bit [20211012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20211012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20211012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20211012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20211012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20211012.170745_fbsd-builder_stable_11]

```

```

JUNOS py extensions [20211017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20211017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20211012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20211012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20211017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20211017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20211017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20211017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20211017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20211017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20211017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20211017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20211017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20211017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20211012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20211017.110007_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 9: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the [Installation and Upgrade Guide](#).

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.

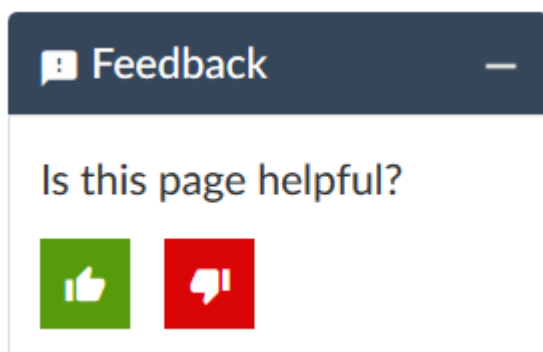
- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#).

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable)

Requesting Technical Support

IN THIS SECTION

- [Self-Help Online Tools and Resources | 270](#)
- [Creating a Service Request with JTAC | 270](#)

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://supportportal.juniper.net/s/knowledge>
- 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://supportportal.juniper.net/s/knowledge>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://supportportal.juniper.net/>

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

Creating a Service Request with JTAC

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

- Visit <https://support.juniper.net/support/requesting-support/>
- 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

20 July 2023—Revision 8, Junos OS Release 21.3R2— ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

2 June 2023—Revision 7, Junos OS Release 21.3R2— ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

25 November 2022—Revision 6, Junos OS Release 21.3R2— ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

4 August 2022—Revision 5, Junos OS Release 21.3R2— ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

29 July 2022—Revision 4, Junos OS Release 21.3R2— ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

24 March 2022—Revision 3, Junos OS Release 21.3R2— ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

7 March 2022—Revision 2, Junos OS Release 21.3R2— ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

24 February 2022—Revision 1, Junos OS Release 21.3R2— ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

25 November 2021—Revision 8, Junos OS Release 21.3R1— ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

12 November 2021—Revision 7, Junos OS Release 21.3R1— ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

28 October 2021—Revision 6, Junos OS Release 21.3R1— ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

18 October 2021—Revision 5, Junos OS Release 21.3R1— ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

14 October 2021—Revision 4, Junos OS Release 21.3R1— ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

1 October 2021—Revision 3, Junos OS Release 21.3R1— ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

30 September 2021—Revision 2, Junos OS Release 21.3R1— ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

23 September 2021—Revision 1, Junos OS Release 21.3R1— ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2023 Juniper Networks, Inc. All rights reserved.