

Release Notes

Published
2023-08-10

Junos® OS Release 21.2R3 for the 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

Table of Contents

Introduction | 1

Junos OS Release Notes for ACX Series

What's New | 2

What's New in 21.2R3 | 2

What's New in 21.2R2 | 2

What's New in 21.2R1 | 2

Dynamic Host Configuration Protocol | 3

Ethernet Switching and Bridging | 3

EVPN | 3

Layer 2 VPN | 4

Multicast | 4

Network Management and Monitoring | 4

Routing Options | 5

Routing Protocols | 5

Source Packet Routing in Networking (SPRING) or Segment Routing | 6

System Management | 6

What's Changed | 7

What's Changed in Release 21.2R3 | 7

What's Changed in Release 21.2R2 | 8

What's Changed in Release 21.2R1 | 8

Known Limitations | 10

Open Issues | 12

Resolved Issues | 13

Resolved Issues: 21.2R3 | 13

Resolved Issues: 21.2R2 | 16

Resolved Issues: 21.2R1 | 18

Documentation Updates | 21

Migration, Upgrade, and Downgrade Instructions | 21

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 21

Junos OS Release Notes for cSRX

What's New | 23

What's New in 21.2R3 | 23

What's New in 21.2R2 | 23

What's New in 21.2R1 | 24

Platform and Infrastructure | 24

What's Changed | 24

What's Changed in Release 21.2R3 | 25

What's Changed in Release 21.2R2 | 25

What's Changed in Release 21.2R1 | 25

Known Limitations | 25

Open Issues | 25

Resolved Issues | 25

Resolved Issues: 21.2R3 | 26

Resolved Issues: 21.2R2 | 26

Resolved Issues: 21.2R1 | 26

Documentation Updates | 26

Junos OS Release Notes for EX Series

What's New | 27

What's New in 21.2R3 | 27

What's New in 21.2R2 | 27

What's New in 21.2R1 | 27

Hardware | 28

EVPN | 42

- Forwarding Options | 43
- IPv6 | 43
- Junos Telemetry Interface | 43
- Licensing | 45
- Network Management and Monitoring | 57
- Routing Options | 57
- Software Installation and Upgrade | 58

What's Changed | 58

- What's Changed in Release 21.2R3 | 59
- What's Changed in Release 21.2R2 | 60
- What's Changed in Release 21.2R1 | 60

Known Limitations | 63

Open Issues | 64

Resolved Issues | 67

- Resolved Issues: 21.2R3 | 67
- Resolved Issues: 21.2R2 | 71
- Resolved Issues: 21.2R1 | 76

Documentation Updates | 82

Migration, Upgrade, and Downgrade Instructions | 82

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 82

Junos OS Release Notes for JRR Series

What's New | 84

- What's New in 21.2R3 | 84
- What's New in 21.2R2 | 84
- What's New in 21.2R1 | 84

What's Changed | 84

- What's Changed in Release 21.2R3 | 85

What's Changed in Release 21.2R2 | 85

What's Changed in Release 21.2R1 | 85

Known Limitations | 85

Open Issues | 85

Resolved Issues | 86

Resolved Issues: 21.2R3 | 86

Resolved Issues: 21.2R2 | 86

Resolved Issues: 21.2R1 | 87

Documentation Updates | 87

Migration, Upgrade, and Downgrade Instructions | 87

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 87

Junos OS Release Notes for Juniper Secure Connect

What's New | 89

What's New in 21.2R3 | 90

What's New in 21.2R2 | 90

What's New in 21.2R1 | 90

What's Changed | 90

What's Changed in Release 21.2R3 | 90

What's Changed in Release 21.2R2 | 90

What's Changed in Release 21.2R1 | 90

Known Limitations | 91

Open Issues | 91

Resolved Issues | 91

Resolved Issues: 21.2R3 | 91

Resolved Issues: 21.2R2 | 92

Resolved Issues: 21.2R1 | 92

Documentation Updates | 92

Junos OS Release Notes for Junos Fusion for Enterprise

What's New | 93

What's New in 21.2R3 | 93

What's New in 21.2R2 | 93

What's New in 21.2R1 | 93

What's Changed | 93

What's Changed in Release 21.2R3 | 94

What's Changed in Release 21.2R2 | 94

What's Changed in Release 21.2R1 | 94

Known Limitations | 94

Open Issues | 94

Resolved Issues | 95

Resolved Issues: 21.2R3 | 95

Resolved Issues: 21.2R2 | 95

Resolved Issues: 21.2R1 | 95

Documentation Updates | 95

Migration, Upgrade, and Downgrade Instructions | 96

Junos OS Release Notes for Junos Fusion for Provider Edge

What's New | 102

What's New in 21.2R3 | 103

What's New in 21.2R2 | 103

What's New in 21.2R1 | 103

What's Changed | 103

What's Changed in Release 21.2R3 | 103

What's Changed in Release 21.2R2 | 103

| What's Changed in Release 21.2R1 | 104

Known Limitations | 104

Open Issues | 104

Resolved Issues | 104

| Resolved Issues: 21.2R3 | 105

| Resolved Issues: 21.2R2 | 105

| Resolved Issues: 21.2R1 | 105

Documentation Updates | 105

Migration, Upgrade, and Downgrade Instructions | 105

Junos OS Release Notes for MX Series

What's New | 115

What's New in 21.2R3 | 116

What's New in 21.2R2 | 116

What's New in 21.2R1 | 116

| Hardware | 117

| Authentication and Access Control | 118

| Flow-Based and Packet-Based Processing | 118

| High Availability | 119

| Interfaces | 119

| Juniper Extension Toolkit (JET) | 120

| Junos Telemetry Interface | 121

| Layer 2 VPN | 122

| MACsec | 122

| MPLS | 123

| Network Address Translation (NAT) | 124

| Network Management and Monitoring | 125

| Platform and Infrastructure | 126

| Routing Options | 126

| Routing Policy and Firewall Filters | 127

| Routing Protocols | 128

| Services Applications | 129

- Software Defined Networking (SDN) | 131
- Software Installation and Upgrade | 132
- Source Packet Routing in Networking (SPRING) or Segment Routing | 132
- Subscriber Management and Services | 133
- System Management | 134

What's Changed | 134

- What's Changed in Release 21.2R3 | 135
- What's Changed in Release 21.2R2 | 137
- What's Changed in Release 21.2R1 | 137

Known Limitations | 142

Open Issues | 146

Resolved Issues | 163

- Resolved Issues: 21.2R3 | 163
- Resolved Issues: 21.2R2 | 179
- Resolved Issues: 21.2R1 | 194

Documentation Updates | 221

Migration, Upgrade, and Downgrade Instructions | 222

Junos OS Release Notes for NFX Series

What's New | 230

- What's New in 21.2R3 | 230
- What's New in 21.2R2 | 230
- What's New in 21.2R1 | 230
 - Application Identification (AppID) | 230
 - Authentication and Access Control | 232
 - Flow-Based and Packet-Based Processing | 232

What's Changed | 232

- What's Changed in Release 21.2R3 | 233
- What's Changed in Release 21.2R2 | 233

| [What's Changed in Release 21.2R1](#) | [233](#)

[Known Limitations](#) | [233](#)

[Open Issues](#) | [233](#)

[Resolved Issues](#) | [235](#)

| [Resolved Issues: 21.2R3](#) | [235](#)

| [Resolved Issues: 21.2R2](#) | [235](#)

| [Resolved Issues: 21.2R1](#) | [236](#)

[Documentation Updates](#) | [237](#)

[Migration, Upgrade, and Downgrade Instructions](#) | [238](#)

[Junos OS Release Notes for PTX Series](#)

[What's New](#) | [241](#)

[What's New in 21.2R3](#) | [241](#)

[What's New in 21.2R2](#) | [241](#)

[What's New in 21.2R1](#) | [241](#)

| [Hardware](#) | [242](#)

| [High Availability](#) | [243](#)

| [Juniper Extension Toolkit \(JET\)](#) | [243](#)

| [Junos Telemetry Interface](#) | [244](#)

| [Layer 2 VPN](#) | [245](#)

| [Network Management and Monitoring](#) | [246](#)

| [Routing Options](#) | [246](#)

| [Routing Policy and Firewall Filters](#) | [247](#)

| [Routing Protocols](#) | [247](#)

| [Services Applications](#) | [248](#)

| [Source Packet Routing in Networking \(SPRING\) or Segment Routing](#) | [248](#)

[What's Changed](#) | [249](#)

| [What's Changed in Release 21.2R3](#) | [250](#)

| [What's Changed in Release 21.2R2](#) | [250](#)

| [What's Changed in Release 21.2R1](#) | [251](#)

Known Limitations | 254

Open Issues | 254

Resolved Issues | 258

Resolved Issues: 21.2R3 | 258

Resolved Issues: 21.2R2 | 261

Resolved Issues: 21.2R1 | 263

Documentation Updates | 268

Migration, Upgrade, and Downgrade Instructions | 268

Junos OS Release Notes for QFX Series

What's New | 273

What's New in 21.2R3 | 274

What's New in 21.2R2 | 274

EVPN | 274

Additional Features | 276

What's New in 21.2R1 | 277

Dynamic Host Configuration Protocol | 277

EVPN | 278

Forwarding Options | 279

High Availability | 279

Interfaces | 279

Juniper Extension Toolkit (JET) | 280

Junos Telemetry Interface | 280

Licensing | 282

Network Management and Monitoring | 283

Routing Options | 284

Routing Protocols | 284

Services Applications | 284

Software Installation and Upgrade | 285

System Management | 285

What's Changed | 285

What's Changed in Release 21.2R3 | 286

What's Changed in Release 21.2R2 | 287

What's Changed in Release 21.2R1 | 287

Known Limitations | 290

Open Issues | 292

Resolved Issues | 299

Resolved Issues: 21.2R3 | 300

Resolved Issues: 21.2R2 | 306

Resolved Issues: 21.2R1 | 312

Documentation Updates | 320

Migration, Upgrade, and Downgrade Instructions | 320

Junos OS Release Notes for SRX Series

What's New | 335

What's New in 21.2R3 | 335

What's New in 21.2R2 | 335

What's New in 21.2R1 | 335

Application Identification (AppID) | 336

Authentication and Access Control | 337

Flow-Based and Packet-Based Processing | 338

Interfaces | 339

J-Web | 339

Juniper Advanced Threat Prevention Cloud (ATP Cloud) | 340

Junos Telemetry Interface | 341

Network Management and Monitoring | 341

Software Installation and Upgrade | 341

Securing GTP and SCTP Traffic | 342

VPNs | 342

What's Changed | 343

What's Changed in Release 21.2R3 | 343

What's Changed in Release 21.2R2 | 345

What's Changed in Release 21.2R1 | 345

Known Limitations | 348

Open Issues | 349

Resolved Issues | 353

Resolved Issues: 21.2R3 | 354

Resolved Issues: 21.2R2 | 360

Resolved Issues: 21.2R1 | 365

Documentation Updates | 370

Migration, Upgrade, and Downgrade Instructions | 370

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 371

Junos OS Release Notes for vMX

What's New | 372

What's New in 21.2R3 | 372

What's New in 21.2R2 | 373

What's New in 21.2R1 | 373

Layer 2 VPN | 373

Routing Options | 373

Routing Protocols | 374

What's Changed | 374

What's Changed in Release 21.2R3 | 374

What's Changed in Release 21.2R2 | 375

What's Changed in Release 21.2R1 | 375

Known Limitations | 376

Open Issues | 376

Resolved Issues | 377

Resolved Issues: 21.2R3 | 377

Resolved Issues: 21.2R2 | 378

Resolved Issues: 21.2R1 | 378

Documentation Updates | 379

Upgrade Instructions | 379

Junos OS Release Notes for vRR

What's New | 380

What's New in 21.2R3 | 380

What's New in 21.2R2 | 380

What's New in 21.2R1 | 380

What's Changed | 380

What's Changed in Release 21.2R3 | 381

What's Changed in Release 21.2R2 | 381

What's Changed in Release 21.2R1 | 381

Known Limitations | 381

Open Issues | 381

Resolved Issues | 382

Resolved Issues: 21.2R3 | 382

Resolved Issues: 21.2R2 | 383

Resolved Issues: 21.2R1 | 383

Documentation Updates | 383

Junos OS Release Notes for vSRX

What's New | 384

What's New in 21.2R3 | 384

What's New in 21.2R2 | 385

What's New in 21.2R1 | 385

Application Identification (AppID) | 385

Flow-Based and Packet-Based Processing | 386

- Platform and Infrastructure | 386
- Securing GTP and SCTP Traffic | 387
- VPNs | 387

What's Changed | 388

- What's Changed in Release 21.2R3 | 388
- What's Changed in Release 21.2R2 | 389
- What's Changed in Release 21.2R1 | 389

Known Limitations | 390

Open Issues | 391

Resolved Issues | 392

- Resolved Issues: 21.2R3 | 393
- Resolved Issues: 21.2R2 | 395
- Resolved Issues: 21.2R1 | 397

Documentation Updates | 398

Migration, Upgrade, and Downgrade Instructions | 399

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 405

Licensing | 406

Finding More Information | 407

Documentation Feedback | 407

Requesting Technical Support | 408

Revision History | 410

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 21.2R3 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 | 7](#)
- [Known Limitations | 10](#)
- [Open Issues | 12](#)
- [Resolved Issues | 13](#)
- [Documentation Updates | 21](#)
- [Migration, Upgrade, and Downgrade Instructions | 21](#)

These release notes accompany Junos OS Release 21.2R3 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 21.2R3 | 2](#)
- [What's New in 21.2R2 | 2](#)
- [What's New in 21.2R1 | 2](#)

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

What's New in 21.2R3

There are no new features or enhancements to existing features for ACX Series in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for ACX Series in Junos OS Release 21.2R2.

What's New in 21.2R1

IN THIS SECTION

- [Dynamic Host Configuration Protocol | 3](#)
- [Ethernet Switching and Bridging | 3](#)
- [EVPN | 3](#)
- [Layer 2 VPN | 4](#)
- [Multicast | 4](#)
- [Network Management and Monitoring | 4](#)
- [Routing Options | 5](#)
- [Routing Protocols | 5](#)
- [Source Packet Routing in Networking \(SPRING\) or Segment Routing | 6](#)
- [System Management | 6](#)

Learn about new features or enhancements to existing features in this release for the ACX Series.

Dynamic Host Configuration Protocol

- **Support for persistent storage of DHCPv4 and DHCPv6 bindings over EVPN IRB (ACX5448, ACX5448-D, and ACX5448-M)**—Starting in Junos OS Release 21.2R1, ACX5448, ACX5448-D, and ACX5448-M routers that are configured to function as a DHCP relay agent can also be configured to preserve the DHCPv4 and DHCPv6 subscriber bindings across reboots. Existing bindings are written to a local file in `/var/preserve`. After reboot, the binding table is populated with the contents of the file, and the router identifies each subscriber that was on the deleted interface, and resumes normal packet processing for subscribers when the interface is restored. To preserve the subscriber binding information, enable the `persistent-storage` statement at the `[edit system services dhcp-local-server]` hierarchy level.

[See [Preserving Subscriber Binding Information](#) and [DHCPv6 Relay Agent Overview](#).]

Ethernet Switching and Bridging

- **Support for L2PT over VPLS networks (ACX710, ACX5448, ACX5448-D, and ACX5448-M)**—Starting in Junos OS Release 21.2R1, we support Layer 2 protocol tunneling (L2PT) over virtual private LAN service (VPLS) networks. The device can use L2PT to transparently send packets across a VPLS network without interfering with protocol instances in the network. L2PT supports 802.1x, 802.3ah, CDP, E-LMI, MVRP, LACP, STP/RSTP/MSTP, LLDP, MMRP, and VTP Layer 2 control protocols.

[See [Layer 2 Protocol Tunneling](#) and [Configuring VPLS Encapsulation on CE-Facing Interfaces](#).]

- **Support for Ethernet Ring Protection (ACX5448, ACX5448-M, and ACX5448-D)**—Starting in Junos OS Release 21.2R1, you can use ERPS to reliably achieve carrier-class network requirements for Ethernet topologies forming a closed loop.

[See [Understanding Ethernet Ring Protection Switching Functionality](#) .]

EVPN

- **Support for DHCP Option 82 over EVPN (ACX Series)**—Starting in Junos OS Release 21.2R1, Option 82 flags are inserted in the DHCP packets to enhance security when the packet is sent to the server. The provider edge (PE) router that is part of the EVPN instance acts as the relay agent, and adds these flags to the DHCP packets.

DHCPv4 packet relay and DHCPv6 packet relay use this process. With the introduction of EVPN IRB, the relay agent uses the IRB interface with EVPN for forwarding the requests, and for replies to and from the client or the server instead of using the default routing option. If one PE router fails, an appropriate DHCPv6-PD state is made available for the remaining PE routers participating in the DHCP-PD process for the VLAN. This is done using automatic synchronization of DHCPv6-PD states

between multiple PE routers that are connected to the same Ethernet segment identifier (ESI) through EVPN BGP messages.

[See [Understanding DHCP Option 82](#)

- **Support for DHCPv6-PD on EVPN IRB synchronization among multiple PE routers (ACX Series)**—You can use DHCPv6 prefix delegation (DHCPv6-PD) to automate the delegation of IPv6 prefixes to a requesting router on EVPN IRB. DHCPv6 prefix delegation is configured on EVPN IRB, and provides IPv6 prefixes to the requesting clients instead of a unique address. The DHCPv6-PD server acts as a provider edge (PE) router that provides the delegates through the relay (PE router) operating in the EVPN instance.

If one PE router fails, an appropriate DHCPv6-PD state is made available for the remaining PE routers participating in the DHCP-PD process for the VLAN. This is done using automatic synchronization of DHCPv6-PD states between multiple PE routers that are connected to the same Ethernet segment identifier (ESI) through EVPN BGP messages.

Layer 2 VPN

- **Pseudowire redundancy support (ACX710)**—Starting in Junos OS Release 21.2R1, the ACX710 routers support pseudowire redundancy in Layer 2 circuits on multichassis link aggregation group (MC-LAG) routers.

[See [Understanding Pseudowire Redundancy Mobile Backhaul Scenarios.](#)]

Multicast

- **Support for BGP MVPN (ACX710 routers)**—Starting in Junos OS Release 21.2R1, ACX710 routers support BGP multicast virtual private network (MVPN) (also known as next-generation (NG) MVPN). You can configure multipoint LDP provider tunnels as the data plane for intra-AS BGP MVPNs. ACX710 routers do not support extranet MVPN.

[See [Multiprotocol BGP MVPNs Overview.](#)]

Network Management and Monitoring

- **Enhanced CFM support (ACX5448, ACX5448-M, and ACX5448-D)**—Starting in Junos OS Release 21.2R1, you can enable the performance monitoring responder functionality without enabling the transmission of continuity check messages (CCM). To enable the performance monitoring responder functionality without enabling CCM transmission, configure our new configuration statement `send-zero-interval-ccm` under the `[edit protocols protocols oam ethernet connectivity-fault-management]` hierarchy level. After you configure the statement, if the continuity-check is not enabled, CCMs are not transmitted, but are programmed to receive the CFM packets for that maintenance endpoint (MEP) level.

[See [IEEE 802.1ag OAM Connectivity Fault Management Overview](#) and [connectivity-fault-management \(EX Series Switch Only\)](#).]

- **Support for port mirroring (ACX710)**—Starting in Junos OS Release 21.2R1, you can use analyzers to mirror copies of packets to a configured destination. You configure the analyzer at the [edit forwarding-options analyzer] hierarchy level.

[See [show forwarding-options analyzer](#).]

Routing Options

- **Enhancements to prefix-limit and accepted-prefix-limit configuration statements, and updates to show bgp neighbor command (ACX1000, EX9200, MX Series, PTX5000, and QFX10002)**— Starting from Junos OS Release 21.2R1, the prefix-limit and accepted-prefix-limit configuration statements include the following options:
 - `drop-excess <percentage>`—If you include the `drop-excess <percentage>` option, the excess routes are dropped when the maximum number of prefixes is reached. If you specify a percentage, the routes are logged when the number of prefixes exceeds that percentage value of the maximum number.
 - `hide-excess <percentage>`—If you include the `hide-excess <percentage>` option, the excess routes are hidden when the maximum number of prefixes is reached. If you specify a percentage, the routes are logged when the number of prefixes exceeds that percentage value of the maximum number.

The `show bgp neighbor` command has been enhanced to display the following additional information:

- Count of prefixes that are dropped or hidden based on network layer reachability information (NLRI) when the maximum allowed prefixes threshold is exceeded.
- Alerts when a peer starts to drop or hide routes.
- Configuration details of the `prefix-limit` and `accepted-prefix-limit` configuration statements.

[See [prefix-limit](#), [accepted-prefix-limit](#), [show bgp neighbor](#), and [Multiprotocol BGP](#).]

Routing Protocols

- **Support for flexible algorithm in IS-IS for segment routing-traffic engineering (ACX Series)**—Starting in Junos OS Release 21.2R1, you can thin slice a network by defining flexible algorithms that compute paths using different parameters and link constraints based on your requirements. For example, you can define a flexible algorithm that computes a path to minimize IGP metric and define another flexible algorithm to compute a path based on traffic-engineering metric to divide the network into separate planes. This feature allows networks without a controller to configure traffic engineering and utilize segment routing capability of a device.

To define a flexible algorithm, include the `flex-algorithm` statement at the [edit routing-options] hierarchy level.

To configure participation in a flexible algorithm include the `flex-algorithm` statement at the [edit protocols isis segment routing] hierarchy level.

[See [Understanding IS-IS Flexible Algorithm for Segment Routing.](#)]

- **Flexible algorithm inter-level leaking support for SRv6 and SR-MPLS in ISIS (ACX Series, MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support flexible algorithm inter-level leaking for SRv6 and SR-MPLS in IS-IS. Also, we partially support TE-App RFC 8919 in its basic form and extends 6PE support for flexible algorithm.

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Support for Layer 3 services over segment routing infrastructure (ACX710 routers)**—Starting in Junos OS Release 21.2R1, ACX710 routers support the following features:
 - IPv4 OSPF segment routing enabled through MPLS.
 - IS-IS segment routing enabled through MPLS.
 - Segment routing–traffic engineering (SR-TE).
 - Segment routing global block (SRGB) range label, which is used by Source Packet Routing in Networking (SPRING).
 - Anycast segment identifiers (SIDs) and prefix SIDs in SPRING.
 - Topology-independent loop-free alternate (TI-LFA) with segment routing, which enables fast rerouting.
 - MPLSlabel stack fast reroute (FRR) backup paths corresponding to the post-convergence path for a given failure.

[See [Understanding Source Packet Routing in Networking \(SPRING\)](#), [Understanding Adjacency Segments, Anycast Segments, and Configurable SRGB in SPRING for IS-IS Protocol](#), and [Understanding Topology-Independent Loop-Free Alternate with Segment Routing for IS-IS.](#)]

System Management

- **G.8275.1 Telecom profile and PTP over Ethernet encapsulation support (ACX2100 and ACX2200)**—Starting in Junos OS Release 21.2R1, ACX2100 and ACX2200 routers support Precision Time Protocol (PTP) over Ethernet encapsulation and G.8275.1 Telecom profile.

The G.8275.1 Telecom profile supports the architecture defined in ITU-T G.8275 to enable the distribution of phase and time with full timing support. This profile requires all devices in the network

to operate in combined or hybrid modes, which means that PTP and Synchronous Ethernet are enabled on all devices.

PTP over Ethernet enables the effective implementation of packet-based technology that enables the operator to deliver synchronization services on packet-based mobile backhaul networks.

[See [G.8275.1 Telecom Profile](#) and [Precision Time Protocol Overview](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3](#) | 7
- [What's Changed in Release 21.2R2](#) | 8
- [What's Changed in Release 21.2R1](#) | 8

Learn about what changed in the Junos OS main and maintenance releases for ACX Series routers.

What's Changed in Release 21.2R3

IN THIS SECTION

- [Interfaces and Chassis](#) | 7
- [Network Management and Monitoring](#) | 8

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

- **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.](#)]

- **Changes to the NETCONF <edit-config> RPC response (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the <edit-config> operation returns an error, the NETCONF server does not emit a <load-error-count> element in the RPC response. In earlier releases, the <edit-config> RPC response includes the <load-error-count> element when the operation fails.

What's Changed in Release 21.2R2

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R2 for ACX Series.

What's Changed in Release 21.2R1

IN THIS SECTION

- [Class of Service \(CoS\) | 9](#)
- [EVPN | 9](#)
- [Junos XML API and Scripting | 9](#)
- [Network Management and Monitoring | 9](#)

Class of Service (CoS)

- Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

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.

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.](#)]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See [request system scripts refresh-from](#) and [cert-file \(Scripts\)](#).]

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.](#)]

- **Changes to <commit> RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server's response for <commit> operations includes the following changes:
 - If a successful <commit> operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.
 - The NETCONF server response emits the <source-daemon> element as a child of the <error-info> element instead of the <rpc-error> element.
 - If you also configure the `flatten-commit-results` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server suppresses any <commit-results> XML subtree in the response and only emits an <ok/> or <rpc-error> element.

[See [Configuring RFC-Compliant NETCONF Sessions.](#)]

- **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.](#)]

See

Known Limitations

IN THIS SECTION

- [General Routing | 11](#)
- [Infrastructure | 11](#)

Learn about known limitations in Junos OS Release 21.2R3 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

- On the ACX710 router, sequential increment of both SRC and DST MAC do not provide better load balance as per HASH result. [PR1477964](#)
- The packet time error on ACX5448 chassis with g.8275.2.enh profile is exceeding class-A time error limits of maximum TE of 100ns. The 1pps time error is exceeding the cTE of 50ns. [PR1535434](#)
- Configuring rib-group to import/export routes across different routing instance is not supported in DNX(ACX5448) platform. These rib-group imported/exported routes will be of type "rtbl"(rtable). To configure this rtable type routes and do route forwarding in hardware, double route lookup support is required. DNX hardware chipset does not support the double route lookup across two different routing tables. Therefore, rib-group route import/export across routing instance is not supported in DNX platform. [PR1547078](#)
- Ping might fail if the MAC address of the device is modified to a static mac address as BCM supports only one base mac address. [PR1553472](#)
- Unified ISSU is not supported from Junos OS earlier releases to Junos OS Release 20.4 and later. There is a major SDK upgrade from 6.3.2 to 6.5.16, because of which the warm boot feature needed for an unified ISSU is not supported by our vendor. [PR1554915](#)
- There is no support for Layer 3 inject in routing instance in ACX5448. BFD packets are Layer 3 injected for PPMAN-based sessions as multihop BFD is PPMAN-based and seeing an issue while transmitting. [PR1569443](#)
- EXP to EXP remarking on PHP router will work for default EXP remarking only. Custom EXP remarking will not work on chip. [PR1640588](#)

Infrastructure

- The image validation is not supported while upgrading from earlier releases to Junos OS Release 21.2 and later. [PR1568757](#)

Open Issues

IN THIS SECTION

- [General Routing | 12](#)

Learn about open issues Junos OS Release 21.2R3 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 show variable latency values. This is expected for host-generated ICMP traffic because of the design of the Packet Forwarding Engine queue polling the packets from ASIC. [PR1380145](#)
- The circuit-cross-connect logs do not compress after rotation. [PR1398511](#)
- 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](#)
- On the ACX710 routers, if the console cable is plugged in and the terminal connection is active and is sending characters to the interface, the system boot might be interrupted and the ACX710 boot will be stalled. [PR1513553](#)
- On the ACX710 routers, alarm does not raise while booting the system with the recovery snapshot. [PR1517221](#)
- On the ACX5448 routers, ping stops working even though the ARP entry is present during continuous script executions. [PR1533513](#)
- The MC-LAG ICL interface needs to be configured as an aggregated Ethernet interface. [PR1567790](#)
- On the ACX448 routers, the packet buffer allocation failed messages appears when you scale the CFM sessions with the SLA iterator. [PR1574754](#)
- Micro-bfd session gets stuck in INIT state at ACX7100 when peer router ACX5448 is used. Micro bfd is not qualified with vlan-tagged configuration on ACX5448. [PR1574780](#)

- On ACX5448 platforms, if hierarchical-scheduler is configured for an interface, during an interface flap or configuration changes, some of Packet Forwarding Engine buffers might not synchronize. As a result, packets might drop without congestion. [PR1603622](#)
- When multihop BFD is configured on ACX5448, delegated BFD sessions are not coming up. [PR1633395](#)
- ACX710 MC-LAG non-revertive function is not working as expected. [PR1633847](#)
- Failing to remove USB stick causing installation to start again. As a workaround, USB installation requires a keypress before reboot to enable removal of USB device before system is restarted. [PR1640143](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.2R3 | 13](#)
- [Resolved Issues: 21.2R2 | 16](#)
- [Resolved Issues: 21.2R1 | 18](#)

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R3

IN THIS SECTION

- [General Routing | 14](#)
- [Platform and Infrastructure | 16](#)

General Routing

- On ACX5448 BFD session status is in INIT state, after system reboot. It is seen when we have both CFM and BFD configured on the system. [PR1552235](#)
- Unknown SMART attributes for StorFly VSF8M8CC200G SSD might be seen on MX10008/MX10016/PTX10008/PTX10016 with JNP10K-RE1. [PR1598566](#)
- On ACX5448 routers, CFM does not appear to be in the Ok state after the router reboots. [PR1602489](#)
- On ACX5096 routers, the pps traffic output appears on the deactivated interfaces. [PR1608827](#)
- On ACX710 routers running Junos OS Release 21.2R1 and later might experience kernel crash. [PR1608852](#)
- On ACX5448 and ACX710 routers, traffic towards the CE device through the default route might be dropped in VRF. [PR1611651](#)
- The maximum entry for ECMP is 4096. If all this is used up due to this stale entries, new ECMP entries cannot be created. Therefore, traffic drop will be seen on ACX5448 and ACX710 [PR1612026](#)
- The routing protocol engine CPU is getting stuck at 100 percent. [PR1612387](#)
- The transit traffic might be impacted on PTP scenario. [PR1612429](#)
- Packet fragmentation might be seen when MTU is configured for logical interface. [PR1614449](#)
- On ACX5448 routers, a warning message: "CHASSISD_GENERIC_WARNING: cfg_ddl_handle_rio_pfe_dfw_profile: New firewall profile configured" is observed. As a workaround, restart the Packet Forwarding Engine. [PR1614512](#)
- On ACX5448 routers, there might be mismatches in statistics at rates above 4GB between the physical and logical interfaces. [PR1614550](#)
- When configuring vlan-id-range/list for an aggregated Ethernet interface of layer 2 circuit, the traffic forwarding is only seen for the first VLAN. [PR1616147](#)
- Traffic might not be forwarded after failover in L2 circuit hot standby mode. [PR1616892](#)
- The PFE daemon crash occurs if the standby interface is disabled in the Layer 2 circuit pseudowire redundancy scenario on ACX710 and ACX5448 platforms. [PR1617287](#)
- Host-outbound-traffic might be placed in incorrect queue. [PR1619174](#)
- Traffic might get equally load-balanced irrespective of the scheduler configuration. [PR1620137](#)
- IGMP: 6-8 seconds delay noticed is seen when the receiver switches in between groups. [PR1620685](#)

- Traffic does not get forwarded to one of the the single-homed PE device after you change the VLAN-ID under the routing instance. [PR1621036](#)
- On ACX5448 and ACX710 routers with Layer 3 VPN scenarios, error messages might be generated after multiple core link or protocol flaps. [PR1621425](#)
- The jnxDomCurrentAlarms value is incorrectly set which might indicate a temperature alarm. [PR1621894](#)
- On ACX5448 routers, the smartd configurations do not get applied. [PR1623359](#)
- COS - EXP rewrite is not working in l3vpn scenario when mf filter is configured. [PR1623922](#)
- On ACX5000 local fault and remote fault signaling is not logged on `/var/log/` messages. [PR1624761](#)
- Unicast packet loss might be observed due to control-word configuration. [PR1626058](#)
- VPLS traffic loss might be observed post route flap. [PR1626267](#)
- Packet Forwarding Engine might crash after device reboot or Packet Forwarding Engine restarts. [PR1626503](#)
- Output packet statistics are not incremented on the unit even after configuring statistics. [PR1627040](#)
- igmp-snooping configuration is dropping l2vpn multicast traffic on ACX Series platform. [PR1628600](#)
- ACX5048 filters reporting TCAM errors are not installed in hardware after the upgrade from Junos OS Release 17.4R2-S8 to Junos OS Release 20.4R3. [PR1630280](#)
- ACX710 running G.8275.2 stuck at PTP acquiring state if the connection is through some timing unaware nodes. [PR1632761](#)
- Speed 10m configuration error on ACX5048 and ACX5096 routers. [PR1633226](#)
- The storm-control rate-limit might not work with VPLS policer under logical interfaces. [PR1633427](#)
- DHCP clients might not come online for IRB+VLAN/EVPN scenario. [PR1633778](#)
- IS-IS last transition time never increments. [PR1634747](#)
- IPv6 BFD session over aggregated Ethernet might stay down on ACX5448 and ACX710 routers. [PR1635020](#)
- The LACP delay might be observed with an "aggregate wait time" of more than 1 second. [PR1635763](#)
- ACX710 and ACX5448 working as PE stops forwarding L3VPN traffic after core-facing link flap. [PR1635801](#)

- ACX5448 PEM overload alarm threshold is incorrect. [PR1636222](#)
- Locally switched traffic might be dropped on ACX5448 with ESI configured. [PR1638386](#)
- The KRT queue might get stuck with the error "ENOMEM -- Cannot allocate memory". [PR1642172](#)

Platform and Infrastructure

- JDI-RCT vRCT : vmxt_lnx core found @ topo_get_link jnh_features_get_jnh jnh_stream_attach. [PR1638166](#)

Resolved Issues: 21.2R2

IN THIS SECTION

- [General Routing | 16](#)
- [Platform and Infrastructure | 17](#)

General Routing

- On ACX5448 router, the two-way time error and CTE for 1 PPS does not meet the class A metrics. [PR1535434](#)
- The DNX router fails to program multicast route in BCM when the route has PIME interface as outgoing interface. [PR1560914](#)
- Inline BFD stays down with IS-IS and static clients. [PR1561590](#)
- The MPC7E, MPC10E, MX-SPC3, and LC2103 line cards might go offline when the device runs on the FIPS mode. [PR1576577](#)
- RLFA does not take effect due to the incorrectly popped service label. [PR1577460](#)
- On ACX5448 routers, asynchronous notification for 1G interface fails to work. [PR1580700](#)
- The rpd process might be stuck at 100 percent due to a race condition. [PR1582226](#)
- On ACX710 routers, unexpected results are observed while verifying channelized interface checks with the SNMP MIB get ifHighSpeed output. [PR1583995](#)
- In a certain condition, PTP might get stuck and does not function properly on ACX710 routers. [PR1587990](#)

- On ACX710 and ACX5400 routers, traffic might get forwarded through the member links in down state after new member links are added to aggregated Ethernet interface. [PR1589168](#)
- On ACX710 and ACX5400 routers running DHCP relay does not process packets arriving over MPLS with an explicit null label. [PR1590225](#)
- Traffic is not passing through the l2circuit interface when the vlan-id-range is configured. [PR1590969](#)
- On ACX5448 routers, high DMR out of sequence is observed with the iterator configuration. [PR1596050](#)
- On ACX710 routers, l2ald core files are seen 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 is observed in an EVPN VPWS flexible cross connect. [PR1598074](#)
- On ACX710 and ACX5448 routers, traffic loss might be observed if the drop-profiles is modified. [PR1598595](#)
- On ACX710 routers, rpf-check-bytes and rpf-check-packets counters are not getting updated properly to flat file as expected. [PR1600513](#)
- On ACX5448 and ACX710 routers, MACsec traffic over Layer 2 circuit might not work. [PR1603534](#)
- The FPC might restart when executing the show firewall command on the ACX5448 platforms. [PR1605288](#)
- The optics_mts_010.robot script fails while verifying SNMP and matching the CLI values. [PR1605348](#)
- On ACX5448 and ACX710 routers running DHCP relay does not process packets arriving over MPLS. [PR1605854](#)
- The Forwarding Engine Board (FEB) might crash on the ACX1000, ACX1100, ACX2000, ACX2100, and ACX4000 platforms. [PR1606424](#)
- The DHCP packets might not be relayed on the ACX710 and ACX5448 platforms. [PR1608125](#)
- The routing protocol engine CPU gets stuck at 100 percent. [PR1612387](#)
- ACX5048 routers places host outbound traffic in a incorrect queue. [PR1619174](#)

Platform and Infrastructure

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

Resolved Issues: 21.2R1

IN THIS SECTION

- [Class of Service \(CoS\) | 18](#)
- [General Routing | 18](#)
- [Routing Protocols | 21](#)

Class of Service (CoS)

- The explicit classifier or rewrite-rule might not work as expected for a logical interface when the configured wildcard. [PR1556103](#)
- FPC might crash might when you issue the `show class-of-service` command. [PR1568661](#)

General Routing

- The IPv6 BFD sessions with configuration below 100 ms flaps. [PR1456237](#)
- The aggregated Ethernet interface with LFM configured might not come up after reboot. [PR1526283](#)
- Packets might drop after configuring the PTP transparent clock. [PR1530862](#)
- On the ACX5448 routers, the BGPV6LU traffic drops when the node gets deployed in ingress. [PR1538819](#)
- In the Layer 3 VPN scenario, the CE device traffic drops on the ingress PE device while resolving using the default route in VRF. [PR1551063](#)
- Verification of multiple PD synchronizations with relay results in the deletion and addition of configurations. [PR1554647](#)
- The ACX5448 or ACX710 router as the TWAMP server delays the start session acknowledgment by 10 seconds. [PR1556829](#)
- On the ACX5448 routers, the unicast packets from the CE devices might be forwarded by the PE devices with an additional VLAN tag if IRB is used. [PR1559084](#)
- On the ACX5448 routers, single rate three color polices does not work. [PR1559665](#)
- On the ACX5048 routers, the fxpc process generates the core file on the analyzer configuration. [PR1559690](#)

- On the ACX2100 routers, laser-output-power occurs after disabling the interface and then rebooting. [PR1560501](#)
- On the ACX5448 routers, the following syslog message gets reported in every 30 seconds:

```
ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_dyn_entry_counter_get : Entry is invalid.
```

[PR1562323](#)

- On the ACX5048 routers, the MAC address entry with no traffic for the MAC age timer does not age out if an active traffic destined for the MAC is available. [PR1565642](#)
- Loopback0 firewall might not take effect along with error logs. [PR1566417](#)
- On the management interface of the ACX5448, ACX5448-D, and ACX5448-M routers, LLDP does not work. [PR1566454](#)
- On the ACX5448 and ACX710 routers, pushing more than 2 MPLS labels might not work. [PR1566828](#)
- The log file of the lcklsyncd process displays empty. [PR1567687](#)
- On the ACX500 routers, service MIC does not work. [PR1569103](#)
- On the ACX5048 routers, traffic-input-pps do not get incremented for VLAN tagged_flexible traffic. [PR1569763](#)
- On the ACX5448 routers, the untagged traffic gets incorrectly queued and marked. [PR1570899](#)
- On the ACX5448 routers, the RFC2544 reflector feature are not able to work on a higher port. [PR1571975](#)
- ARP traffic exceeding the polices limit does not get discarded. [PR1573956](#)
- Packets might get tagged with default VLAN-ID and dropped at the peer under the Layer 2 circuits local switching scenario. [PR1574623](#)
- The ACX Series router fails to process the RSVP path message. [PR1576585](#)
- Committing scheduler-map under class-of-service displays the following error message:

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

[PR1579009](#)

- On the ACX710 routers, configuration under auxiliary port causes continuous reboot. [PR1580016](#)

- An ACX router that runs DHCP Relay does not process packets received from the DHCP server if the packets arrive over MPLS with an explicit null label. [PR1590225](#)
- Traffic does not pass through circuit cross-connect interface with configured VLAN-ID range. [PR1590969](#)
- Packets might drop with all the commit events with the 1G speed configured interface. [PR1524614](#)
- On the ACX710 routers, unexpected results are observed while verifying the channelized interface check with the snmp mib get ifHighSpeed output. [PR1583995](#)
- On the ACX5448 routers, detection time shows the default value (6.000) instead of the configured value for a single hop BFD. [PR1585382](#)
- On the ACX710 routers, the size of the jnpr-clock-recovery.log log file is small and the archives rotate too quickly. [PR1582350](#)
- On the ACX710 routers, the l2ald process generates the 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](#)
- BUM traffic might be dropped in the VPLS instance under certain conditions. [PR1531733](#)
- On the ACX5448 router, the SFP-T interface might not come up if a straight cable is used. [PR1547394](#)
- When an RDI is received with CCM packet, sessions do not get deleted. [PR1560182](#)
- When the LACP daemon restarts, the LACP local partner system ID remains 0 in the mc-ae output. [PR1560820](#)
- Analyzer (Port Mirroring) might not work on ports above 20. [PR1563774](#)
- The DF (Designated Forwarder) might not forward traffic. [PR1567752](#)
- ACX routers reset the tunable optics to the default wavelength after an upgrade or reboot. [PR1570192](#)
- The l2circuit and CFM sessions might go down when you configure the asynchronous-notification. [PR1572722](#)
- On the ACX5448 and ACX710 routers, 802.1P rewrite might not work. [PR1574601](#)
- There might be a traffic drop between the customer edge and provider edge devices in case of the ARP resolution failure. [PR1580782](#)
- On the ACX710 and ACX5448 routers, DHCPv4 might not work. [PR1589135](#)

- On the ACX5448 and ACX710 routers, traffic drop occurs in the EVPN VPWS flexible cross connect. [PR1598074](#)

Routing Protocols

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

Documentation Updates

There are no corrections or changes in Junos OS Release 21.2R3 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](#) | 21

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 21.2R3, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

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

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

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

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

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

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

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 1: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for cSRX

IN THIS SECTION

- [What's New | 23](#)
- [What's Changed | 24](#)
- [Known Limitations | 25](#)

- Open Issues | 25
- Resolved Issues | 25
- Documentation Updates | 26

These release notes accompany Junos OS Release 21.2R3 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 21.2R3 | 23
- What's New in 21.2R2 | 23
- What's New in 21.2R1 | 24

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

What's New in 21.2R3

There are no new features or enhancements to existing features for cSRX Series in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for cSRX Series in Junos OS Release 21.2R2.

What's New in 21.2R1

IN THIS SECTION

- [Platform and Infrastructure | 24](#)

Learn about new features or enhancements to existing features in this release for cSRX.

Platform and Infrastructure

- **cSRX support on AWS (cSRX)**—Starting in Junos OS Release 21.2R1, you can deploy cSRX Container Firewall in Amazon Web Services (AWS) Cloud using Amazon Elastic Kubernetes Services (Amazon EKS), which is a fully managed Kubernetes service.

With cSRX, you can also set up automated service provisioning and orchestration, distributed and multitenant traffic security, centralized management with Juniper® Security Director (including dynamic policy and address update, remote log collections, security events monitoring), and scalable security services with small footprints.

cSRX is available with 60 days free trial eval license (S-CSRX-A1 SKU). The eval license in cSRX expires after 60 days.

You can purchase bring your own license (BYOL) from Juniper Networks or a Juniper Networks authorized reseller for using the software features on the cSRX. Use this license to customize your license, subscription, and support.

[See [cSRX Deployment Guide for AWS](#) and [Flex Software License for cSRX](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 25](#)
- [What's Changed in Release 21.2R2 | 25](#)
- [What's Changed in Release 21.2R1 | 25](#)

Learn about what changed in the Junos OS main and maintenance releases for cSRX.

What's Changed in Release 21.2R3

There are no changes in behavior and syntax in Junos OS Releases 21.2R3 for cSRX.

What's Changed in Release 21.2R2

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R2 for cSRX.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for cSRX.

Known Limitations

There are no known limitations in hardware or software in Junos OS Release 21.2R3 for cSRX.

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

Open Issues

There are no known issues in hardware or software in Junos OS Release 21.2R3 for cSRX.

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

Resolved Issues

IN THIS SECTION

● [Resolved Issues: 21.2R3 | 26](#)

● [Resolved Issues: 21.2R2 | 26](#)

- [Resolved Issues: 21.2R1 | 26](#)

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R3

There are no resolved issues in Junos OS Releases 21.2R3 for cSRX.

Resolved Issues: 21.2R2

There are no resolved issues for cSRX in Junos OS Release 21.2R2.

Resolved Issues: 21.2R1

There are no resolved issues for cSRX in Junos OS Release 21.2R1.

Documentation Updates

There are no corrections or changes in Junos OS Release 21.2R3 documentation for cSRX.

Junos OS Release Notes for EX Series

IN THIS SECTION

- [What's New | 27](#)
- [What's Changed | 58](#)
- [Known Limitations | 63](#)
- [Open Issues | 64](#)
- [Resolved Issues | 67](#)
- [Documentation Updates | 82](#)

- [Migration, Upgrade, and Downgrade Instructions | 82](#)

These release notes accompany Junos OS Release 21.2R3 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 21.2R3 | 27](#)
- [What's New in 21.2R2 | 27](#)
- [What's New in 21.2R1 | 27](#)

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

What's New in 21.2R3

There are no new features or enhancements to existing features for EX Series Switches in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for EX Series Switches in Junos OS Release 21.2R2.

What's New in 21.2R1

IN THIS SECTION

- [Hardware | 28](#)

- [EVPN | 42](#)
- [Forwarding Options | 43](#)
- [IPv6 | 43](#)
- [Junos Telemetry Interface | 43](#)
- [Licensing | 45](#)
- [Network Management and Monitoring | 57](#)
- [Routing Options | 57](#)
- [Software Installation and Upgrade | 58](#)

Learn about new features or enhancements to existing features in this release for EX Series Switches.

Hardware

IN THIS SECTION

- [EX4400-24MP and EX4400-48MP Features | 29](#)

- The following methods to protect the chassis from excessive current draw and temperature conditions are supported:
 - Configure Junos OS to automatically shut down the PSM, or raise an alarm and log the event when a field-effect transistor (FET) failure is detected in the power supply module (PSM) by using the specified command. [See [thermal-health-check](#)].
 - Configure upgrade of the PSM firmware that will take action when there is an FET failure by using the specified command. [See [request system firmware upgrade](#)].
 - Configure Junos OS to raise an alarm and log events when a PSM with upgraded firmware version shuts down due to an FET failure, Junos OS on the attached device.
 - Configure a monitor to check how much power the chassis draws from the PSM using the specified command. If the system draws more power from the PSM than what it should consume, Junos OS raises an alarm or shuts down the system. [See [watchdog \(PSM\)](#)].
[See [Handling Thermal Health Events Using Thermal Health Check and PSM Watchdog](#)].

- Support for CLD LED (EX4400 switches)—In Junos OS Release 21.2R1, we have enabled the Cloud LED on EX4400 switches. The feature is under development. To learn more about the LED, see [EX4400 Switch Hardware Guide](#).

EX4400-24MP and EX4400-48MP Features

We've added the following features to the EX4400-24MP and EX4400-48MP switches in Junos OS Release 21.2R1.

- **Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches**

Feature	Description
Hardware	<ul style="list-style-type: none"> • New EX4400 switch models—In Junos OS Release 21.2R1, we introduce the following new models of the EX4400 switch: EX4400-24MP and EX4400-48MP. The EX4400-24MP model has 24 100-Mbps, 1-Gbps, 2.5-Gbps, 5-Gbps, or 10-Gbps RJ-45 ports on the front panel. The EX4400-48MP model has 36 100-Mbps, 1-Gbps, or 2.5-Gbps RJ-45 ports and 12 100-Mbps, 1-Gbps, 2.5-Gbps, 5-Gbps, or 10-Gbps RJ-45 ports on the front panel. These ports support IEEE 802.3bt Power over Ethernet (PoE-bt). The EX4400 switches provide connectivity for high-density environments and scalability for growing networks. <p>Typically, EX4400 switches are used in large branch offices, campus wiring closets, and data centers.</p> <p>In data centers, you can position EX4400 switches as top-of-rack switches to provide connectivity for all devices in the rack. EX4400 switches are our first cloud-ready switches. You can deploy EX4400 switches in cloud networks and manage them by using Juniper Mist Wired Assurance. EX4400-24MP switches support 1050-W AC power supplies. EX4400-48MP switches support 1600-W AC power supplies. EX4400 switches support front-to-back or back-to-front airflow directions.</p> <p>EX4400 switches support channelization. [See Port Settings.]</p> <p>To install the EX4400 switch hardware and perform initial software configuration, routine maintenance, and troubleshooting, see EX4400 Switch Hardware Guide. See Feature Explorer for the complete list of features for any platform.</p>
Authentication and access control	<ul style="list-style-type: none"> • 802.1X authentication. [See 802.1X Authentication.] • Captive portal. [See Captive Portal Authentication.]

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches (Continued)

Feature	Description
Chassis	<ul style="list-style-type: none"> • PSU, fan, and temperature sensors are monitored as part of chassis FRU management and environment support for multi-rate switch. <p>PSU management includes redundancy support and power budgeting.</p> <p>Fan management includes speed change based on ambient temperature.</p> <p>Temperature sensor monitoring provides periodic temperature sensor data for the smooth functioning of switch. When the temperature reported by various sensors crosses the specified threshold, then the fan speed increases or decreases. If the shutdown threshold is breached, then system shutdown is initiated.</p> <p>[See EX4400 Switch Hardware Guide.]</p>
Class of service	<ul style="list-style-type: none"> • Support for Class of Service (CoS) configuration <p>[See Class of Service User Guide (EX Series Switches Except EX4600 and EX9200 Switches).]</p>

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description
EVPN	<ul style="list-style-type: none"> • Layer 3 VXLAN gateway in EVPN-VXLAN centrally routed bridging overlay or edge-routed bridging overlay networks is supported on standalone switches or a Virtual Chassis, and includes the following features: <ul style="list-style-type: none"> • Default gateway using IRB interfaces to route traffic between VLANs. [See Using a Default Layer 3 Gateway to Route Traffic in an EVPN-VXLAN Overlay Network.] • IPv6 data traffic routed through an EVPN-VXLAN overlay network with an IPv4 underlay. [See Routing IPv6 Data Traffic through an EVPN-VXLAN Network with an IPv4 Underlay.] • EVPN pure Type 5 routes. [See Understanding EVPN Pure Type-5 Route.] <p>The Virtual Chassis doesn't support EVPN-VXLAN multihoming, but you can use the standalone switch as an EVPN-VXLAN provider edge device in multihoming use cases.</p> • Enhancement in the number of supported VLANs and ports—We have increased the combined total number of VLANs and ports that can be supported on the EX4400 switches. The number of supported VLANs remains at 4093, but Junos OS no longer limits the total number of ports and VLANs that can be configured on EVPN-VXLAN. This enhancement applies only when you use the enterprise style of configuration while configuring the interfaces. <p>[See Understanding EVPN with VXLAN Data Plane Encapsulation.]</p> • Support for the following Layer 2 VXLAN gateway features in an EVPN-VXLAN network: <ul style="list-style-type: none"> • Active/active multihoming • Proxy ARP use and ARP suppression, and Neighbor Discovery Protocol (NDP) use and NDP suppression on non-IRB interfaces • Ingress node replication for broadcast, unknown unicast, and multicast (BUM) traffic forwarding <p>[See EVPN Feature Guide.]</p> • Support for Layer 2 VXLAN gateway services in an EVPN-VXLAN network: <ul style="list-style-type: none"> • 802.1X authentication, accounting, CWA authentication, and captive portal

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches (Continued)

Feature	Description
	<ul style="list-style-type: none"> • CoS • DHCPv4 and DHCPv6 snooping, dynamic ARP inspection (DAI), neighbor discovery inspection, IP source guard and IPv6 source guard, and router advertisement (RA) guard (no multihoming) • Firewall filters and policing • Storm control, port mirroring, and MAC filtering <p>[See EVPN Feature Guide.]</p>
High Availability	<ul style="list-style-type: none"> • High availability includes NSSU, GRES, NSB, and NSR. [See High Availability User Guide.]

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches (Continued)

Feature	Description
Interfaces	<ul style="list-style-type: none"> • Support for multi-rate ports on EX4400-24MP and EX4400-48MP switches that support higher scale and bandwidth. <p>The EX4400-48MP switch contains a total of 48 ports, of which:</p> <ul style="list-style-type: none"> • 36 ports (0-35) operate at 2.5-Gbps, 1-Gbps, and 100-Mbps speed. • 12 ports (36-47) operate at 10-Gbps, 5-Gbps, 2.5-Gbps, 1-Gbps, and 100-Mbps speed. <p>The EX4400-24MP switch contains 24 ports that operate at 10-Gbps, 5-Gbps, 2.5-Gbps, 1-Gbps, and 100-Mbps speed.</p> <p>Both the switches support the following four-port extension modules. However, you can install only one module at a time in the chassis:</p> <ul style="list-style-type: none"> • The native extension module EX4400-EM-4Y supports 25-Gbps speed. • The other extension module EX4400-EM-4S supports 10-Gbps speed. <p>[See Channelizing Interfaces on EX4400 Switches.]</p> <ul style="list-style-type: none"> • Support for optics Forward Error Correction (FEC) sensor diagnostics, interfaces node level failure and restoration, and logging of operational, administrative events, and errors. Support for laser output and laser receiver power management. <p>[See Troubleshoot the EX4400 Components.]</p> <ul style="list-style-type: none"> • Support for the IEEE 802.3bt standard for Power over Ethernet (PoE) and fast PoE— With fast PoE enabled, the switch saves PoE power settings across a reboot, and powers on the powered device (PD) at the initial stage of the boot (within a few seconds of switching on power) before the complete switch is booted. To configure fast PoE, use the command <code>set poe fast-poe</code>. [See Understanding PoE on EX Series Switches.]

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description
Junos Telemetry Interface	<ul style="list-style-type: none"> • JTI Packet Forwarding Engine and Routing Engine sensor support—Use the Junos telemetry interface (JTI) and remote procedure calls (gRPC) to stream statistics from the switches to an outside collector. <p>The following Routing Engine statistics are supported:</p> <ul style="list-style-type: none"> • LACP state export • Chassis environmentals export • Network discovery chassis and components • LLDP export and LLDP model • BGP peer information (RPD) • RPD task memory utilization export • Network discovery ARP table state • Network discovery NDP table state <p>The following Packet Forwarding Engine statistics are supported:</p> <ul style="list-style-type: none"> • Congestion and latency monitoring • Logical interface • Filter • Physical interface • NPU/LC memory • Network discovery NDP table state <p>To provision a sensor to export data through gRPC, use the telemetry Subscribe RPC to specify telemetry parameters.</p> <p>[See Configuring a Junos Telemetry Interface Sensor (CLI Procedure), Configure a NETCONF Proxy Telemetry Sensor in Junos, and Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).]</p>

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches (Continued)

Feature	Description
	<ul style="list-style-type: none"> Secure packet capture to cloud—We support secure packet capture using Junos telemetry interface (JTI). You can use this feature to capture packets from a device and send them over a secure channel to an external collector (in the cloud) for monitoring and analysis. The maximum size of the packet you can capture is 128 bytes, including the packet header and the data within. Network professionals use real-time packet capture data to troubleshoot complex issues such as network and performance degradation and poor end-user experience. <p>To use secure packet capture, include the <code>/junos/system/linecard/packet-capture</code> resource path using a Junos RPC call.</p> <p>For ingress packet capture, include the <code>packet-capture</code> option in the existing firewall filter configuration at the <code>[edit firewall family <i>family-name</i> filter <i>filter-name</i> term <i>match-term</i> then packet-capture]</code> hierarchy level. Do this before you send packet capture sensor data to the collector and remove the <code>packet-capture</code> configuration after data is sent to the collector. After the capture is done, ingress packets with the filter match conditions are trapped to the CPU. The trapped packets then go to the collector over a secure channel in JTI-specified format in key-value pairs by means of Remote Procedure Call (gRPC) transport.</p> <p>For egress packet capture on physical interfaces (<code>ge-*</code>, <code>xe-*</code>, <code>mge-*</code>, and <code>et-*</code>), include "packet-capture-telemetry," "egress," and "interface <interface-name>" at the <code>[edit forwarding-options]</code> hierarchy level. For example:</p> <pre>set forwarding-options packet-capture-telemetry egress interface ge-0/0/0 set forwarding-options packet-capture-telemetry egress interface mge-0/0/10</pre> <p>You can add multiple interfaces on the device for egress packet capture. When configured, host-bound egress packets are captured from the interface and sent to the collector. As with the ingress configuration, remove the configuration when packet capture is not required.</p>

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches (Continued)

Feature	Description
Layer 2 Features	<ul style="list-style-type: none"> • The following Layer 2 unicast features are supported on EX4400-24MP and EX4400-48MP switches: <ul style="list-style-type: none"> • 802.1D • 802.1w (RSTP) • 802.1s (MST) • BPDU protect • Loop protect • Root protect • VSTP • 802.1Q VLAN trunking • 802.1p • PVLAN • Routed VLAN Interface (RVI) • Layer 3 VLAN-tagged subinterfaces • 4096 VLAN support • Multiple VLAN Registration Protocol (802.1ak) • MAC address filtering • MAC address aging configuration • Static MAC address assignment for interface • Per VLAN MAC learning (limit) • MAC learning disable • Persistent MAC (sticky MAC)

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches (Continued)

Feature	Description
	<ul style="list-style-type: none"> • Link aggregation static and dynamic with LACP (fast and slow LACP) • LLDP • Uplink failure detection (UFD) • VXLAN Layer 2 gateway (EVPN) • Ethernet ring protection switching (ERPS) version 1 comprises the following Layer 2 features: <ul style="list-style-type: none"> • Revertive mode of operation of the Ethernet ring • Multiple ring instances on the same interfaces • Multiple ring instances on different interfaces • Interworking with Spanning Tree Protocol, Multiple Spanning Tree Protocol, and redundant trunk groups <p>[See Ethernet Ring Protection Switching Overview.]</p>

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches (Continued)

Feature	Description
Layer 3 Features	<ul style="list-style-type: none"> • The following Layer 3 unicast features are supported on EX4400-24MP and EX4400-48MP switches: <ul style="list-style-type: none"> • BFD for RIP, OSPF, ISIS, BGP, PIM • BGP 4-byte ASN support • BGP Add Path (BGP-AP) • Filter-based forwarding (FBF) • IP-directed broadcast traffic forwarding • IS-IS • IPv4 BGP • IPv4 MBGP • IPv4 over GRE • IPv6 BGP • IPv6 CoS (BA, classification and rewrite, scheduling based on TC) • IPv6 IS-IS • IPv6 OSPFv3 • IPv6 ping • IPv6 stateless auto-configuration • IPv6 static routing • IPv6 traceroute • OSPFv2 • Path MTU discovery • RIPv2

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches (Continued)

Feature	Description
	<ul style="list-style-type: none"> • Static routing • Unicast reverse path forwarding (unicast RPF) • Virtual router for ISIS, RIP, OSPF, and BGP • Virtual Router Redundancy Protocol (VRRP) • VRRPv3 • 32-way equal-cost multipath (ECMP) <p>[See BGP User Guide, Routing Policies, Firewall Filters, and Traffic Policers User Guide, IS-IS User Guide, Security Services Administration Guide, and OSPF User Guide.]</p>
Multicast	<ul style="list-style-type: none"> • IGMP snooping • IGMP: version 1, version 2, version 3 • Multicast Listener Discovery (MLD) snooping • PIM-SM, PIM-SSM, PIM-DM <p>[See Multicast Protocols User Guide.]</p>
Network management and monitoring	<ul style="list-style-type: none"> • Local and remote port mirroring, and remote port mirroring to an IP address (GRE encapsulation). [See Port Mirroring and Analyzers.] • sFlow network monitoring technology. [See sFlow Monitoring Technology.]
Routing policy and firewall filters	<ul style="list-style-type: none"> • Firewall filters and policers. [See Firewall Filters Overview.]

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches (Continued)

Feature	Description
Security	<ul style="list-style-type: none"><li data-bbox="477 373 1393 436">• Support for Media Access Control Security (MACsec) with 256-bit cipher suite. [See Understanding Media Access Control Security (MACsec).]<li data-bbox="477 472 1016 499">• Support for the following port security features:<ul style="list-style-type: none"><li data-bbox="513 535 886 562">• DHCP snooping (IPv4 and IPv6)<li data-bbox="513 598 870 625">• Dynamic ARP inspection (DAI)<li data-bbox="513 661 919 688">• IPv6 neighbor discovery inspection <p data-bbox="513 724 987 751">[See Security Services Administration Guide.]</p>

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description
Software Installation and Upgrade	<ul style="list-style-type: none"> • Support for the phone-home client—The phone-home client (PHC) can securely provision an EX4400 Virtual Chassis without requiring user interaction. You only need to: <ul style="list-style-type: none"> • Ensure that the Virtual Chassis members have the factory-default configuration. • Interconnect the member switches using dedicated or default-configured Virtual Chassis ports. • Connect the Virtual Chassis management port or any network port to the network. • Power on the Virtual Chassis members. <p>The PHC automatically starts up on the Virtual Chassis and connects to the phone-home server (PHS). The PHS responds with bootstrapping information, including the Virtual Chassis topology, software image, and configuration. The PHC upgrades each Virtual Chassis member with the new image and applies the configuration, and the Virtual Chassis is ready to go.</p> <p>[See Provision a Virtual Chassis Using the Phone-Home Client.]</p> • ZTP with IPv6 support—You can use a DHCPv6 client and zero-touch provisioning (ZTP) to provision a device. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding the image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If one of the DHCPv4 bindings fails, the device continues to check for bindings until provisioning is successful. However, if there are no DHCPv4 bindings, the device checks for DHCPv6 bindings and follows the same process as for DHCPv4 until the device is provisioned successfully. Both DHCPv4 and DHCPv6 clients are included as part of the default configuration on the device. <p>The DHCP server uses DHCPv6 options 59 and 17 and applicable suboptions to exchange ZTP-related information between itself and the DHCP client.</p> <p>[See Zero Touch Provisioning.]</p> • Support for DHCP option 43 suboption 8 to provide proxy server information in PHC —During the bootstrapping process, the phone-home client (PHC) can access the redirect server or the phone-home server through a proxy server. The DHCP server uses DHCP option 43 suboption 8 or DHCP option 17 suboption 8 to deliver the details of both IPv4 and IPv6 proxy servers to the PHC. The DHCP daemon running on the target switch learns about the proxy servers in the initial DHCP cycle. The

Table 2: Features Supported by the EX4400-24MP and EX4400-48MP Switches (Continued)

Feature	Description
	<p>daemon then populates either the phc_vendor_specific_info.xml files or the phc_v6_vendor-specific_info.xml files located at <code>/var/etc/</code> with vendor-specific information.</p> <p>[See Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client.]</p>
Virtual Chassis	<ul style="list-style-type: none"> Virtual Chassis support for all EX4400 switch models. You can connect up to 10 EX4400 switches in a Virtual Chassis, and manage them as a single device. <p>[See EX4400 Switches in a Virtual Chassis.]</p>

EVPN

- **Port-based VLAN bundle services for EVPN (EX9200)**—Starting in Junos OS Release 21.2R1, Junos OS supports port-based VLAN bundle services for EVPN on the EX9200 switch. The port-based VLAN bundle service maps the VLANs on a port to the same bundle service.

[See [VLAN Bundle Service for EVPN.](#)]

- **EVPN Type 2 and Type 5 route coexistence (EX4650, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we support the coexistence of EVPN Type 2 and Type 5 routes in EVPN-VXLAN edge-routed bridging overlay fabrics. This feature enables more efficient traffic flow and better usage of Packet Forwarding Engine resources. The switch applies a preference algorithm when you enable Type 5 routes. For any destinations for which the switch has no Type 5 route, the switch uses Type 2 routes by default. Otherwise, the switch gives preference to:

- Type 2 routes for local ESI interfaces (locally learned routes)
- Type 5 routes for all other destinations within the data center or across data centers

You can refine these preferences by configuring routing policies in the EVPN routing instance to control the Type 5 routes that the switch imports and exports.

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

- **Enhancement in the number of supported VLANs and ports (EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, and EX4400-48T switches)**—Starting with Junos OS Release 21.2R1, we have increased the combined total number of VLANs and ports that can be supported on the EX4400 switches. The number of supported VLANs remains at 4093, but Junos OS no longer limits

the total number of ports and VLANs that can be configured on EVPN-VXLAN. This enhancement applies only when you use the enterprise style of configuration when configuring the interfaces.

[See [Understanding EVPN with VXLAN Data Plane Encapsulation.](#)]

Forwarding Options

- **Remote port mirroring with VXLAN encapsulation (EX4650, QFX5120-32C, QFX5120-48T, and QFX5120-48Y switches)**—Starting in Junos OS Release 21.2R1, you can configure remote port mirroring in an EVPN-VXLAN environment. Remote port mirroring sends copies of packets to an output destination for remote monitoring. This feature supports VXLAN encapsulation of the mirrored packets so they can be sent to an output destination in a separate virtual network identifier (VNI) domain.

IPv6

- **Stateless address autoconfiguration (SLAAC) snooping over a Layer 2 EVPN-VXLAN gateway (EX4300-MP and EX4300-MP VC)**—Starting in Junos OS Release 21.2R1, you can enable SLAAC snooping on EX4300-MP switches in an Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) deployment. We support SLAAC snooping on CE-facing L2 interfaces. IPv6 clients using SLAAC for dynamic address assignment are validated against the SLAAC snooping binding table before being allowed access to the network.

[See [IPv6 Stateless Address Auto-configuration \(SLAAC\) Snooping.](#)]

Junos Telemetry Interface

NOTE: For Routing Engine telemetry sensors supported by this platform, see [Telemetry Sensor Explorer](#). If any Platform Forwarding Engine sensors have been added for this release, they are listed below

- **End-of-message notification for Routing Engine sensors (EX2300, EX4300, EX4300-MP, EX9200, MX240, MX960, MX10016, MX2010, MX2020, PTX1000, PTX3000, PTX10001, QFX5100, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we've introduced an end-of-message (EoM) Boolean flag for all Junos telemetry interface (JTI) Routing Engine sensors. The flag notifies the collector that the current wrap has completed for a particular sensor path. A wrap is a complete key-value data dump for all the leaves under a sensor path.

The EoM flag also enables the collector to detect when the end of wrap occurs without having to compare stream creation timestamp values that the collector receives from the packets. Comparing timestamp values is costly time-wise and delays data aggregation.

To use this feature with gRPC Network Management Interface (gNMI) transport or Remote Procedure Call (gRPC), retrieve the protobuf files from the relevant branch on the [Juniper Networks](#) download site:

- GnmJuniperTelemetryHeaderExtension.proto (gNMI)
- agent.proto (for gRPC)

For example: <https://github.com/Juniper/telemetry/blob/master/20.3/20.3R1/protos/GnmJuniperTelemetryHeaderExtension.proto>.

After you download and install the new protobuf files on a collector, the EoM field is present in the packets received.

[See [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **Secure packet capture to cloud (EX4400)**—Starting in Junos OS Release 21.2R1, we support secure packet capture using Junos telemetry interface (JTI). You can use this feature to capture packets from a device and send them over a secure channel to an external collector (in the cloud) for monitoring and analysis. The maximum size of the packet you can capture is 128 bytes, including the packet header and the data within. Network professionals use real-time packet capture data to troubleshoot complex issues such as network and performance degradation and poor end-user experience.

To use secure packet capture, include the `/junos/system/linecard/packet-capture` resource path using a Junos RPC call.

For ingress packet capture, include the `packet-capture` option in the existing firewall filter configuration at the `[edit firewall family family-name filter filter-name term match-term then packet-capture]` hierarchy level. Do this before you send packet capture sensor data to the collector and remove the `packet-capture` configuration after data is sent to the collector. After the capture is done, ingress packets with the filter match conditions are trapped to the CPU. The trapped packets then go to the collector over a secure channel in JTI-specified format in key-value pairs by means of Remote Procedure Call (gRPC) transport.

For egress packet capture on physical interfaces (`ge-*`, `xe-*`, `mge-*`, and `et-*`), include "packet-capture-telemetry," "egress," and "interface <interface-name>" at the `[edit forwarding-options]` hierarchy level.

For example:

```
set forwarding-options packet-capture-telemetry egress interface ge-0/0/0
```

```
set forwarding-options packet-capture-telemetry egress interface ge-0/0/10
```

You can add multiple interfaces on the device for egress packet capture. When configured, host-bound egress packets are captured from the interface and sent to the collector. As with the ingress configuration, remove the configuration when packet capture is not required.

Licensing

- **Juniper Agile Licensing (EX2300, EX3400, EX4300, and EX4400)**—Starting in Junos OS Release 21.2R1, the listed EX Series switches support Juniper Agile Licensing.

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

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

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

[Table 3 on page 46](#) describes the licensing support for soft-enforced features on EX2300 switches.

Table 3: Licensed Features on EX2300 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	<ul style="list-style-type: none"> • Layer 2 and Layer 3 filters • Layer 2 (xSTP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operation, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis*

Table 3: Licensed Features on EX2300 switches (Continued)

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	<ul style="list-style-type: none"> • Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRP version 3 • Multicast Source Discovery protocol (MSDP) • OAM and Maintenance CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • VRRP

Virtual Chassis*—We've included Virtual Chassis license in the Standard license model on EX2300-C 12-port switches. However, we don't include the Virtual Chassis license on EX2300 24-port and 48-port switch models. You need to purchase the license separately.

[Table 4 on page 48](#) describes the licensing support for soft-enforced features on EX3400 switches.

Table 4: Licensed Features on EX3400 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	<ul style="list-style-type: none"> • Layer 2 and Layer 3 filters • Layer 2 (xSTP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 4: Licensed Features on EX3400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	<ul style="list-style-type: none"> • Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRP version 3, and virtual router support for unicast • Filter-based forwarding (FBF) • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 4: Licensed Features on EX3400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Premium	Campus and access Layer 3	<ul style="list-style-type: none"> • Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRPv3, virtual router support for unicast, and FBF • Multicast Source Discovery Protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP • BGP and multiprotocol BGP (MBGP) • IS-IS

Table 5 on page 51 describes the licensing support for soft-enforced features on EX4300 switches.

Table 5: Licensed Features on EX4300 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	<ul style="list-style-type: none"> • Layer 2 and Layer 3 filters • Layer 2 (xSTP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 5: Licensed Features on EX4300 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	<ul style="list-style-type: none"> • Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • FBF • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 5: Licensed Features on EX4300 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Premium	Campus and access Layer 3	<ul style="list-style-type: none"> • Bidirectional Forwarding Detection (BFD) • CFM (IEEE 802.1ag) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery Protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • FBF • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP • BGP and multiprotocol BGP (MBGP) • IS-IS • EVPN-VXLAN <ul style="list-style-type: none"> • Supported only on EX4300-48MP switch. • Requires the BGP for configuration.

Table 6 on page 54 describes the licensing support for soft-enforced features on EX4400 switches.

Table 6: Licensed Features on EX4400 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	<ul style="list-style-type: none"> • Layer 2 and Layer 3 filters • Layer 2 (xSTP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 6: Licensed Features on EX4400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	<ul style="list-style-type: none"> • Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • FBF • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 6: Licensed Features on EX4400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Premium	Campus and access Layer 3	<ul style="list-style-type: none"> • Bidirectional Forwarding Detection (BFD) • CFM (IEEE 802.1ag) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery Protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • FBF • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP • BGP and multiprotocol BGP (MBGP) • IS-IS • EVPN-VXLAN <ul style="list-style-type: none"> • Requires the BGP for configuration.

On EX4400 switch, the flow-based telemetry and MACsec features are hard-enforced. You'll need a license to use these features.

[See [Flex Software License for EX Series Switches](#), [Juniper Agile Licensing Guide](#), and [Configuring Licenses in Junos OS](#).]

Network Management and Monitoring

- **Support for syslog over TLS (EX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, you can transport syslog (control plane) over Transport Layer Security (TLS) protocol. Encapsulating syslog over 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
- 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.

Routing Options

- **Enhancements to prefix-limit and accepted-prefix-limit configuration statements, and updates to show bgp neighbor command (ACX1000, EX9200, MX Series, PTX5000, and QFX10002)**— Starting from Junos OS Release 21.2R1, the `prefix-limit` and `accepted-prefix-limit` configuration statements include the following options:
 - `drop-excess <percentage>`—If you include the `drop-excess <percentage>` option, the excess routes are dropped when the maximum number of prefixes is reached. If you specify a percentage, the routes are logged when the number of prefixes exceeds that percentage value of the maximum number.
 - `hide-excess <percentage>`—If you include the `hide-excess <percentage>` option, the excess routes are hidden when the maximum number of prefixes is reached. If you specify a percentage, the routes are logged when the number of prefixes exceeds that percentage value of the maximum number.

The `show bgp neighbor` command has been enhanced to display the following additional information:

- Count of prefixes that are dropped or hidden based on network layer reachability information (NLRI) when the maximum allowed prefixes threshold is exceeded.
- Alerts when a peer starts to drop or hide routes.

- Configuration details of the `prefix-limit` and `accepted-prefix-limit` configuration statements.

[See [prefix-limit](#), [accepted-prefix-limit](#), [show bgp neighbor](#), and [Multiprotocol BGP](#).]

Software Installation and Upgrade

- **Support for DHCP option 43 suboption 8 to provide proxy server information in PHC (EX2300-C, EX2300-MP, EX4300, EX4300-MP, EX4300-VC, EX4600-VC, EX4650, and EX4650-48Y-VC)**—Starting in Junos OS Release 21.2R1, during the bootstrapping process, the phone-home client (PHC) can access the redirect server or the phone-home server through a proxy server. The DHCP server uses DHCP option 43 suboption 8 or DHCP option 17 suboption 8 to deliver the details of both IPv4 and IPv6 proxy servers to the PHC. The DHCP daemon running on the target switch learns about the proxy servers in the initial DHCP cycle. The daemon then populates either the `phc_vendor_specific_info.xml` files or the `phc_v6_vendor_specific_info.xml` files located at `/var/etc/` with vendor-specific information.

[See [Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client](#).]

- **ZTP with IPv6 support (EX2300-C, EX2300-MP, EX4300, EX4300-MP, EX4300-VC, EX4600-VC, EX4650, and EX4650-48Y-VC)**—Starting in Junos OS Release 21.2R1, you can use a DHCPv6 client and zero-touch provisioning (ZTP) to provision a device. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding the image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If one of the DHCPv4 bindings fails, the device continues to check for bindings until provisioning is successful. However, if there are no DHCPv4 bindings, the device checks for DHCPv6 bindings and follows the same process as for DHCPv4 until the device is provisioned successfully. Both DHCPv4 and DHCPv6 clients are included as part of the default configuration on the device.

The DHCP server uses DHCPv6 options 59 and 17 and applicable suboptions to exchange ZTP-related information between itself and the DHCP client.

[See [Zero Touch Provisioning](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3](#) | 59
- [What's Changed in Release 21.2R2](#) | 60

- [What's Changed in Release 21.2R1 | 60](#)

Learn about what changed in the Junos OS main and maintenance releases for EX Series switches.

What's Changed in Release 21.2R3

IN THIS SECTION

- [Network Management and Monitoring | 59](#)

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.](#)]
- **Changes to the NETCONF `<edit-config>` RPC response (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<edit-config>` operation returns an error, the NETCONF server does not emit a `<load-error-count>` element in the RPC response. In earlier releases, the `<edit-config>` RPC response includes the `<load-error-count>` element when the operation fails.

What's Changed in Release 21.2R2

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R2 for EX Series.

What's Changed in Release 21.2R1

IN THIS SECTION

- [Class of Service \(CoS\) | 60](#)
- [EVPN | 60](#)
- [General Routing | 61](#)
- [Interfaces and Chassis | 61](#)
- [Junos XML API and Scripting | 61](#)
- [Network Management and Monitoring | 62](#)

Class of Service (CoS)

- Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

EVPN

- **IGMP snooping options has changed hierarchy level**–Junos OS has moved the following options from the edit protocols igmp-snooping hierarchy to edit protocols igmp-snooping vlan <vlan-name/vlan-all> hierarchy and edit routing-instances evpn protocols igmp-snooping hierarchy to edit routing-instances evpn protocols igmp-snooping vlan <vlan-name/vlan-all> hierarchy:
 - query-interval
 - query-last-member-interval
 - query-response-interval
 - robust-count
 - evpn-ssm-reports-only
 - immediate-leave

- **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.

General Routing

- **Configure internal IPsec authentication algorithm (EX Series)**—You can configure the algorithm `hmac-sha-256-128` at the `edit security ipsec internal security-association manual direction bidirectional authentication algorithm` hierarchy level for internal IP security (IPsec) authentication. In earlier releases, you could configure the algorithm `hmac-sha-256-128` for MX Series devices only.

Interfaces and Chassis

- **Blocking duplicate IP detection in the same routing instance (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, and SRX Series)**—Junos OS will no longer accept duplicate IPs between different logical interfaces in the same routing instance. Refer to the table mentioned in the topic `inet (interfaces)`. When you try to configure same IP on two logical interfaces inside same routing instance, the commit will be blocked with the error displayed as shown below: `edit user@host# set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.2/24, edit user@host# commit commit complete, edit user@host# set interfaces ge-0/0/2 unit 0 family inet address 2.2.2.2/24 , edit user@host# commit, and edit interfaces ge-0/0/2 unit 0 family inet 'address 2.2.2.2/24' identical local address found on rt_inst default, intfs ge-0/0/2.0 and ge-0/0/1.0, family inet. error: configuration check-out failed`

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.](#)]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See [request system scripts refresh-from](#) and [cert-file \(Scripts\)](#).]

Network Management and Monitoring

- **Chef and Puppet support removed (EX Series except EX4400, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, Junos OS products that were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS. FreeBSD 12.x based Junos OS does not support installing existing Chef or Puppet packages.
- **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](#).]

- **Changes to `<commit>` RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server's response for `<commit>` operations includes the following changes:
 - If a successful `<commit>` operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.
 - The NETCONF server response emits the `<source-daemon>` element as a child of the `<error-info>` element instead of the `<rpc-error>` element.
 - If you also configure the `flatten-commit-results` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server suppresses any `<commit-results>` XML subtree in the response and only emits an `<ok/>` or `<rpc-error>` element.

[See [Configuring RFC-Compliant NETCONF Sessions](#).]

- **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](#) | 63
- [Infrastructure](#) | 64

Learn about known limitations in Junos OS Release 21.2R3 for EX Series switches.

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

General Routing

- Junos OS might hang trying to acquire the SMP IPI lock while rebooting when it is running as a VM on Linux and QEMU hypervisor. [PR1385970](#)
- On a virtual chassis, CLI command to add license is not available on the backup member. Licenses must be added from the primary member only. [PR1545075](#)
- Packets mirrored through analyzer with ingress and egress interfaces across different virtual chassis members might have a different VLAN-ID from that of VLAN-ID of the exiting egress interface. This limitation is from underlying hardware. [PR1552905](#)
- **Resource deadlock avoided** messages observed during software add on EX4400 platforms. No functionality impact seen. [PR1557468](#)
- 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](#)

Infrastructure

- On EX4400 device, a cloud LED on the device indicates the phone home client states and device connectivity state with the cloud. When the grpc application is configured with non-root user, then, the cloud LED will not display any pattern related to day1 states. The LED pattern will still be displaying the previous day0 state as applicable. [PR1589321](#)

Open Issues

IN THIS SECTION

- [General Routing | 64](#)
- [Forwarding and Sampling | 65](#)
- [Infrastructure | 66](#)
- [Platform and Infrastructure | 66](#)
- [User Interface and Configuration | 66](#)

Learn about open issues Junos OS Release 21.2R3 for EX Series switches.

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

General Routing

- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. [PR1362609](#)
- On the EX9214 device, if the MACsec-enabled link flaps after reboot, the error `errorlib_set_error_log(): err_id(-1718026239)` is observed. [PR1448368](#)
- When running 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](#)
- A delay of 35 seconds is added in reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. [PR1514364](#)

- The rpd process might crash and generate a core file when the telemetry data for a streamed node is deleted during a network churn. The same node is being walked or rendered for the sensor. In this corner case the rendering and deletion of a particular node occurs at the same instance. This issue can occur only in case of an unstable network. [PR1552816](#)
- Traffic drops during unified ISSU due to LAG interface flap. [PR1569578](#)
- On a EX4400 VC, the SNMP MIB object `jnRedundancySwitchOverCount` will display the number of times the mastership of the Routing Engine that is changed between primary and backup roles. This counter will not be reset to 0 when entire VC is rebooted. The count displayed under `jnRedundancySwitchOverCount` will be the cumulative value of the switchover events. [PR1570359](#)
- In EVPN_VXLAN deployment, BUM (Broadcast, Unknown Unicast, and Multicast) traffic replication over VTEP might send out more packets than expected. [PR1570689](#)
- On all Junos OS platforms, traffic loss might be observed because of the 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](#)
- Pause frames counters are not getting incremented when pause frames are sent. [PR1580560](#)
- On EX Series switches such as EX2300, EX3400, EX4300, EX4600, and EX4650 with broadcom 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. The following is the product list of EX Series switches with broadcom chip as the Packet Forwarding Engine. [PR1595823](#)
- There is a remote possibility that during many reboots, the Junos VM goes into a state where NMI is needed to continue the reboot. There is no workaround for this and a subsequent reboot does not seem to hit this issue. [PR1601867](#)

Forwarding and Sampling

- The configuration statement `fast-lookup-filter` with match condition is not supported in FLT hardware and might cause a traffic drop. [PR1573350](#)

Infrastructure

- A double free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Refer <https://kb.juniper.net/JSA11162> for more information. [PR1497768](#)
- On a EX4400 device, the CLI command `show system processes detail` will not display CPU details under the CPU column. This issue is fixed from software version 21.3R1 onwards. [PR1588150](#)
- On a EX4400 device, a cloud LED on the device indicates the phone home client states and device connectivity state with the cloud. When the `grpc` application is configured with non root user, then the cloud LED will not display any pattern related to day1 states. The LED pattern will still be displaying the previous day0 state as applicable. [PR1589321](#)

Platform and Infrastructure

- On EX4300 POE switches, the `pfex` process CPU utilization becomes high after 6-8 weeks. There is no functional impact. [PR1453107](#)
- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect ASIC programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. [PR1530160](#)
- On EX9200 line of switches, the FPC gets restarted and thereby disrupts traffic when there is an out-of-order filter state and terms. This issue might be seen only in back-to-back GRES in more than 40 to 50 iterations. [PR1579182](#)
- When a EX4400 Virtual Chassis is scaled with different features configurations and device is stressed with traffic, device might not respond for CLI commands for a short period of time and a `vmcore` might be reported at that time. Once VM core is saved, device will continue to operate normally. [PR1599498](#)
- On all EX4300 platforms(Except EX4300-MP), local fault insertion is failing when the fault is injected (through a traffic generator) and traffic loss is seen on the port. [PR1623215](#)

User Interface and Configuration

- The issue is seen on EX-series VC only which can be avoided with a simple workaround as to providing a valid package during upgrade command. [PR1557628](#)

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.2R3 | **67**
- Resolved Issues: 21.2R2 | **71**
- Resolved Issues: 21.2R1 | **76**

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R3

IN THIS SECTION

- General Routing | **68**
- Class of Service (CoS) | **70**
- High Availability (HA) and Resiliency | **70**
- Interfaces and Chassis | **70**
- Junos Fusion Enterprise | **70**
- Layer 2 Ethernet Services | **70**
- MPLS | **71**
- Platform and Infrastructure | **71**
- Routing Protocols | **71**
- Subscriber Access Management | **71**
- Virtual Chassis | **71**

General Routing

- During flooding, MAC is learnt only on normal access port but not on the aggregated Ethernet interface trunk port. [PR1506403](#)
- In Junos OS **et-** interface stuck and remains down between two particular ports. [PR1535078](#)
- MAC addresses might not be relearned successfully after MAC address age is timed out. [PR1567723](#)
- The upgrade of the PoE firmware might fail on EX2300 and EX3400. [PR1584491](#)
- Inconsistent statistics value seen in slaac-snooping. [PR1590926](#)
- The l2alm fails to send IPC message to the l2ald which might cause the FPC to crash. [PR1596615](#)
- Error message **error: syntax error: request-package-validate** will be seen on device CLI output during Non Stop Software Upgrade. [PR1596955](#)
- The interface on SFP-T or SFP-SX might stop forwarding traffic on EX4600. [PR1598805](#)
- During day1 stage of EX4400 device management from MIST, the cloud LED will remain in green state even if device loses connectivity with cloud. [PR1598948](#)
- The l2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable. [PR1599094](#)
- On EX4300 platform MAC addresses aging issue is seen. [PR1600029](#)
- The SFP-T port might stop forwarding traffic on EX4600 platforms. [PR1600291](#)
- On a EX4400 POE supported device, PoE firmware upgrade should be done with bt-firmware CLI option only. [PR1606276](#)
- Traffic loss might be observed if dot1X is configured with **supplicant multiple** and authenticated user from radius is in single supplicant mode. [PR1610746](#)
- Inter-vlan connectivity might be lost in an EVPN-VXLAN with CRB topology. [PR1611488](#)
- Traffic stops when traffic is switching from one LAG member to another member in case of MACSEC is configured. [PR1611772](#)
- Change in commit error message while configuring the same vlan-id with different vlan-name through openconfig CLI. [PR1612566](#)
- On EX2300, EX3400, EX4300-MP, and EX4400 series is causing MAC move when the IGMP query packet received on backup FPC port. [PR1612596](#)
- Removing the optical module **JNP-SFPP-10GE-T** from a port might cause certain ports to go down. [PR1614139](#)

- Packet Forwarding Engine might crash due to deletion of storm control configuration for IFL in CLI which might lead to traffic loss. [PR1616646](#)
- Core dumps might be seen on EX devices after configuration changes. [PR1618352](#)
- OAM CFM adjacency is not forming on EX4300. [PR1619231](#)
- The process dcpfe might crash after performing VXLAN VNI configuration change and delete on EX series platforms. [PR1619445](#)
- On Junos OS EX2300 Series, EX2300-MP Series, EX3400 Series, a slow memory leak due to processing of specific IPv6 packets (CVE-2022-22180). [PR1619970](#)
- OAM CFM session doesn't come UP if ERPS configured and CFM control traffic uses the same VLAN as ERPS control traffic [PR1620536](#)
- EVPN type 5 routes might not be installed. [PR1620808](#)
- Traffic loss might be observed after configuring VXLAN over IRB interface. [PR1625285](#)
- 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](#)
- When clients connected to isolated VLAN (Virtual Local Area Network) through trunk port cannot communicate to the network. [PR1626710](#)
- Packet drop might be observed when L2PT is configured on transit device. [PR1627857](#)
- The error message **BCM_PVLAN_UTILS:ERR:pfe_bcm_pvlan_utils_get_sec_bd(),789: Failed to get Secondary-bd** is logged when received a dhcp packet on private VLAN. [PR1630553](#)
- 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](#)
- Traffic loss for 20 seconds on VC with aggregated Ethernet link-protection when rebooting backup FPC. [PR1633115](#)
- The VCPs connected with the AOC cable might not come up after upgrading to 17.3 or later releases. [PR1633998](#)
- IRB traffic drop might be observed when mac-persistence-timer expires. [PR1636422](#)
- Configuring L2PT on a transit switch in a Q-in-Q environment breaks L2PT for other S-VLANs. [PR1637249](#)
- MAC address might not be learned on the new interface after MAC move. [PR1637784](#)
- 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](#)
- The error message `dot1xd : devrt_rtsock Don't know how to handle message type 2` is logged even if dot1x is not set. [PR1641304](#)
- In rare scenarios, the EX platform might observe VMcore. [PR1641988](#)

Class of Service (CoS)

- The dcpfe core might be seen in auto-channelization scenario or when SFP is plugged out. [PR1616847](#)
- Memory usage continuously increase is observed on backup chassis if subscriber service is enabled. [PR1595238](#)

High Availability (HA) and Resiliency

- During unified ISSU package signature validation might fail and the upgrade might not happen. [PR1575680](#)

Interfaces and Chassis

- SNMP_TRAP_LINK_UP & SNMP_TRAP_LINK_DOWN trap might be seen while activating and deactivating firewall filters. [PR1609838](#)
- The vrrpd core might be observed after interface state change. [PR1646480](#)

Junos Fusion Enterprise

- On a rare corner case, anchor IFL is not created in time which results in assert core during SD provisioning state. [PR1555597](#)
- There might be memory leak observed in Junos Fusion satellite device for cpd process. [PR1577977](#)

Layer 2 Ethernet Services

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

MPLS

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

Platform and Infrastructure

- Some interfaces might be down after the power outage or power cycle. [PR1580829](#)
- Route leak from primary routing-instance to custom routing-instance failure occurs for local interface. [PR1623429](#)
- The ARP resolution might get failed on VRRP enabled interface. [PR1630616](#)
- Application of firewall filters might break connectivity towards the hosts on EX4300. [PR1630935](#)
- The Packet Forwarding Engine might get crash when VC member flaps on EX platforms. [PR1634781](#)

Routing Protocols

- The rpd core might be observed due to memory corruption. [PR1599751](#)
- The rpd might crash and restart when NSR is enabled. [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 IFDs are attached or detached. [PR1622283](#)
- Delay might be observed while establishing the virtual-chassis post upgrading or rebooting device. [PR1624850](#)

Resolved Issues: 21.2R2

IN THIS SECTION

- [General Routing | 72](#)
- [EVPN | 74](#)

- Infrastructure | 74
- Interfaces and Chassis | 74
- Junos Fusion Enterprise | 75
- Layer 2 Ethernet Services | 75
- Platform and Infrastructure | 75
- Routing Protocols | 75
- Virtual Chassis | 75

General Routing

- MPPE-Send or Recv-key attribute is not extracted correctly by dot1xd. [PR1522469](#)
- On EX Series line of switches Virtual Chassis (VC), Power over Ethernet (POE) might not be detected and hence might fail to work on VC members. [PR1539933](#)
- The Virtual Chassis Port (VCP) might not come up in EX4600 line of switches. [PR1555741](#)
- A few transmitting packets might be dropped because the disable-pfe-action command 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 Series line of switches, the new primary Routing Engine post switchover might go into DB mode (or crash). [PR1565213](#)
- The 40G DAC connection between EX9253 and the peers might not come up. [PR1569230](#)
- Private VLAN configuration might fail in certain scenario. [PR1574480](#)
- The dcpfe crash is observed on Junos OS EX Series line of switches. [PR1578859](#)
- On the EX Series line of switches, a few 40G ports might not be channelized successfully. [PR1582105](#)
- USB boot with image gets stuck and unable to boot the device. [PR1582592](#)
- Packet drops during VRRP primary reboot when 40XS linecard is present on some EX9204 platforms. [PR1586740](#)
- 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](#)
- 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 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 aggregate Ethernet interface as the underlay interface. [PR1592133](#)
- On all Junos OS 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 label field for the EVPN Type 1 route is set to 1. [PR1594981](#)
- 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](#)
- The l2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable. [PR1599094](#)
- 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 Junos OS 20.2 or later, either using phone-home feature or when the system is in factory default state. Upgrading might fail crashing the phone-home feature. [PR1601722](#)
- On EX2300 VC platforms ARP might not get resolved. [PR1602003](#)

- On 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 switches, 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 EX4400 POE supported device, POE firmware upgrade should be done with bt-firmware CLI option only. [PR1606276](#)
- On EX Series switches, the fxpc process might crash and generate a core dump. [PR1607372](#)
- On EX4300 platform, the dcpfe process might crash and generate a core file. [PR1608306](#)
- DHCP packets might be received and then returned back to DHCP relay through the same interface on EX2300, EX3400, and EX4300 Virtual Chassis platforms. [PR1610253](#)
- Change in commit error message while configuring the same vlan-id with different vlan-name through openconfig CLI. [PR1612566](#)
- OAM Connectivity Fault Management adjacency is not forming on EX4300. [PR1619231](#)
- EVPN type 5 routes might not be installed. [PR1620808](#)
- If subscriber service is enabled, the memory usage continuously increases on backup chassis. [PR1595238](#)

EVPN

- Traffic loss might be seen under EVPN-VxLAN scenario when MAC-IP moves from one CE interface to another. [PR1591264](#)
- On all Junos OS platforms, 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

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

Interfaces and Chassis

- ARP resolution failure might occur during VRRP failover. [PR1578126](#)

Junos Fusion Enterprise

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

Layer 2 Ethernet Services

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

Platform and Infrastructure

- Upon receipt of specific sequences of genuine packets destined to the device, the kernel will crash and restart (vmcore). [PR1557881](#)
- The pfex might crash during PIC 4x 1G/10G SFP/SFP+ offline or online. [PR1582457](#)
- 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](#)
- When you configure `mac-move-limit` statement, forwarding the VRRP packet is not possible. [PR1601005](#)
- Adding aggregated Ethernet configuration without child member might cause MAC/ARP learning issues. [PR1602399](#)
- The ZTP service might not work and the image installation might fail. [PR1603227](#)
- Slaac-Snooping global address entry learnt over vtep interface does not RENEW sometimes after lease timer expiry. [PR1603269](#)

Routing Protocols

- 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](#)

Resolved Issues: 21.2R1

IN THIS SECTION

- [Class of Service \(CoS\) | 76](#)
- [Forwarding and Sampling | 76](#)
- [General Routing | 76](#)
- [High Availability \(HA\) and Resiliency | 79](#)
- [Infrastructure | 79](#)
- [Interfaces and Chassis | 80](#)
- [Layer 2 Ethernet Services | 80](#)
- [Layer 2 Features | 80](#)
- [Platform and Infrastructure | 80](#)
- [Routing Protocols | 81](#)
- [User Interface and Configuration | 81](#)
- [Virtual Chassis | 81](#)

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](#)

Forwarding and Sampling

- Configuration archive transfer-on-commit fails when running Junos OS Release 18.2R3-S6.5. [PR1563641](#)

General Routing

- When you rename a Virtual Chassis, the SNMP POE MIB walk produce either no results or sometimes show result from the primary Virtual Chassis. [PR1503985](#)
- The OSPF neighborhood gets stuck in the Start state after configuring the EVPN-VXLAN. [PR1519244](#)
- Packet drops with all commit events with 1G speed configured interface. [PR1524614](#)
- High EVENTD CPU utilization upon receiving LLMNR and MDNS traffic on EX2300. [PR1544549](#)

- The device might be out of service after configuring the em1 or em2 interface. [PR1544864](#)
- Two Routing Engines might lose communication if they have different Junos OS versions on MX10003 and EX Series switches. [PR1550594](#)
- "Cattle-Prod Daemon received unknown trigger (type Semaphore, id 1)" error messages are seen on the vty when the CLI commands to fetch host route scale are issued. [PR1554140](#)
- OIR of CBs might result in major errors and the Packet Forwarding Engine disable action halted traffic forwarding on the FPCs. [PR1554145](#)
- The link on the Linux based LC is not brought down immediately after the FPC process(ukern/indus.elf) crashes or the process is killed [PR1554430](#)
- Traffic might be dropped when a firewall filter rule uses the then VLAN action. [PR1556198](#)
- FPC with power related faults might get on-lined again once Fabric Healing has off-lined the FPC. [PR1556558](#)
- On the EX4300 device, script fails while committing the IPSec authentication configuration as the algorithm statement is missing. [PR1557216](#)
- The MAC addresses learned in a Virtual Chassis might fail due to aging out in the MAC scaling environment. [PR1558128](#)
- The rpd process generates a core file after the Routing Engine switchover. [PR1558814](#)
- 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 tunable optics SFP+-10G-T-DWDM-ZR does not work on EX Series devices. [PR1561181](#)
- When dot1x server-fail-voip vlan-name is configured, ensure that both server-fail-voip vlan-name and voip vlan are configured using vlan-name and not by using vlan-id. [PR1561323](#)
- When you open the configuration database, "Could not open configuration database during usb upgrading" error is seen. [PR1561741](#)
- EX3400VC - SMARTD pollutes syslog every 5 seconds after the upgrade or when the system reboots. [PR1562396](#)
- If a license key has features that are not applicable on the platform (unknown features), the license key is rejected. If the license key has one or more platform applicable features (known features) along with unknown features, license key addition is successful with LICENSE_INVALID_FEATURE_ID syslog warning message for the unknown features. [PR1562700](#)
- On EX3400-VC line of switches, the DAEMON-7-PVIDB throws syslog messages for every 12 to 14 minutes after you upgrade to Junos OS Release 19.1R3-S3. [PR1563192](#)

- Client authentication is failing after performing GRES. [PR1563431](#)
- The JWeb upgrade might fail on EX2300 and EX3400 line of switches. [PR1563906](#)
- The DHCP client might not obtain IP address when dhcp-security is configured [PR1564941](#)
- The Packet Forwarding Engine telemetry data might not be streamed out in EX Series Virtual Chassis. [PR1566528](#)
- On EX4600 platform, internal comment 'Placeholder for QFX Series platform configuration' might be seen on performing `show config` CLI command. [PR1567037](#)
- RPD core file is generated when the device reboots and the daemon restarts. No service impact is observed when the daemon restarts using the routing protocol. [PR1567043](#)
- EX2300 shows high FPC CPU usage. [PR1567438](#)
- The Designated Forwarder (DF) might not forward traffic. [PR1567752](#)
- The 40G DAC connection between EX9253 and the peers might not come up. [PR1569230](#)
- Packet loss might be observed when sample based action is used in firewall filter. [PR1571399](#)
- Port-mirroring might not work when the analyzer output is a trunk interface. [PR1575129](#)
- 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](#)
- MVR configuration cannot be configured on EX2300-C switches. [PR1577905](#)
- The fxpc process might crash on EX Series platforms. [PR1578421](#)
- Random/silent reboot might be seen on EX2300-24MP/EX2300-48MP platforms. [PR1579576](#)
- 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](#)
- After performing NSSU, "timeout waiting for response from fpc0" error message is seen while checking version details. [PR1584457](#)
- DSCP rewriting might fail to work on EX2300 switches. [PR1586341](#)

- The reserved multicast traffic (224.0.0.0/24) might be dropped if IGMP-snooping with pdu-block-on-edge is configured. [PR1586970](#)
- The SNMP trap for MAC notifications might not be generated when an interface is added explicitly under switch-options. [PR1587610](#)
- 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](#)
- Inconsistent statistics value is seen on performing slaac-snooping. [PR1590926](#)
- The LLDP packet might loose on the EX-4300MP platform if LLDP is configured on the management interface. [PR1591387](#)
- The show pfe filter hw command might generate the following error message:

```
ERROR (dfw): Unknown group id: 21
```

[PR1592096](#)

- xSTP might not get configured when enabled on a interface with SP style configuration on all platforms. [PR1592264](#)
- On the EX4400 chassis supporting POE, the show poe controller command might not show details of any POE firmware available for upgrade. You must manually perform a POE firmware upgrade during downtime to upgrade to the latest firmware if packaged with current software version installed on the device. [PR1598766](#)

High Availability (HA) and Resiliency

- The ksyncd core file might be observed while applying the configuration to a logical interface. [PR1551777](#)

Infrastructure

- On the EX4300 Virtual Chassis or Virtual Chassis Fan, HEAP malloc(0) is detected. [PR1546036](#)
- Traffic related to IRB interface might be dropped when mac-persistence-timer expires. [PR1557229](#)
- Traffic might not be forwarded on EX3400 and EX4300mp platforms with Layer 2 classifier rules applied. [PR1561263](#)
- Some MAC addresses might not be aged out on EX4300 platforms. [PR1579293](#)

Interfaces and Chassis

- The pppd might crash when VRRP is configured on all Junos OS or EVO platforms. [PR1561281](#)
- MC-AE interfaces might go down if same VRRP group-id is configured on multiple IRB units. [PR1575779](#)
- The aggregate Ethernet interface might flap. [PR1576533](#)
- VRRP incorrect advertisement threshold values are seen on VRRP groups when VRRP is configured on EX2300 boxes. [PR1584499](#)

Layer 2 Ethernet Services

- An aggregated Ethernet interface flap might be seen during NSSU. [PR1551925](#)
- The DHCP client will be offline for 120 seconds after sending the DHCPINFORM message in the DHCP relay scenario. [PR1575740](#)

Layer 2 Features

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

Platform and Infrastructure

- On the EX3400 Virtula Chassis, you cannot perform console access on the backup Virtual Chassis member. [PR1530106](#)
- Packets transiting through multicast-based VXLAN VTEP interface might be dropped post FPC restart. [PR1536364](#)
- The targeted-broadcast feature might send out duplicate packets. [PR1553070](#)
- The traffic might be dropped on Layer 3 LAG after rebooting or halting any member of EX4300 VC. [PR1556124](#)
- The LLDP neighbor advertisement on EX4300 might send an incorrect 802.3 power format with TLV length 7 instead of length Layer 2. [PR1563105](#)
- The last flapped timestamp for interface fxp0 resets every time when you perform `monitor traffic interface fxp0`. [PR1564323](#)
- When you enable the soft error recovery feature on Packet Forwarding Engine, the PFEX might crash. [PR1567515](#)

- On all EX9200 platforms with EVPN-VXLAN configured, the next-hop memory leak in MX Series ASIC occurs when 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](#)
- Introduce two new major CMERRORs for XM chip-based line card to stabilize the running device. [PR1574631](#)
- DHCP packets with source IP as link-local address drop in EX4300. [PR1576022](#)
- 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](#)

Routing Protocols

- The pcmd memory leak might cause traffic loss. [PR1561850](#)
- The rpd process might crash if there are more routes changed during the commit-sync processing window. [PR1565814](#)
- The untagged packets might not work on EX Series platforms. [PR1568533](#)
- BGP session carrying VPNv4 prefix with IPv6 next-hop might be dropped. [PR1580578](#)
- The rpd might crash in scaled routing instances scenario. [PR1590638](#)

User Interface and Configuration

- The J-Web application cannot be auto-updated for all the supported EX Series devices. [PR1563588](#)

Virtual Chassis

- On the EX4600 and the EX4300 line of switches mixed Virtual Chassis, the following error message appears when you change the configuration related to interface:

```
'ex_bcm_pic_eth_uint8_set
```

[PR1573173](#)

- 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 21.2R3 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](#) | 82

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 21.2R3, 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. EX4400 still runs on FreeBSD 11.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 7: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/Downgrade to subsequent 3 releases	Upgrade/Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	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 | 84](#)
- [What's Changed | 84](#)
- [Known Limitations | 85](#)
- [Open Issues | 85](#)
- [Resolved Issues | 86](#)
- [Documentation Updates | 87](#)
- [Migration, Upgrade, and Downgrade Instructions | 87](#)

These release notes accompany Junos OS Release 21.2R3 for the JRR Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

- [What's New in 21.2R3 | 84](#)
- [What's New in 21.2R2 | 84](#)
- [What's New in 21.2R1 | 84](#)

Learn about new features introduced in the Junos OS main and maintenance releases for JRR Series Route Reflectors.

What's New in 21.2R3

There are no new features or enhancements to existing features for JRR Series Route Reflectors in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for JRR Series Route Reflectors in Junos OS Release 21.2R2.

What's New in 21.2R1

There are no new features or enhancements to existing features for JRR Series Route Reflectors in Junos OS Release 21.2R1.

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 85](#)

- [What's Changed in Release 21.2R2 | 85](#)
- [What's Changed in Release 21.2R1 | 85](#)

Learn about what changed in Junos OS main and maintenance releases for JRR Series Route Reflectors.

What's Changed in Release 21.2R3

There are no changes in behavior and syntax in Junos OS Releases 21.2R3 for JRR Series.

What's Changed in Release 21.2R2

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R2 for JRR Series.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for JRR Series.

Known Limitations

There are no known limitations in hardware or software in Junos OS Release 21.2R3 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 21.2R3 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: 21.2R3 | 86](#)
- [Resolved Issues: 21.2R2 | 86](#)
- [Resolved Issues: 21.2R1 | 87](#)

Learn which issues were resolved in the Junos OS main and maintenance releases for JRR 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: 21.2R3

IN THIS SECTION

- [General Routing | 86](#)

General Routing

- On JRR200, `monitor traffic interface operational` command does not work on em2. [PR1629242](#)

Resolved Issues: 21.2R2

IN THIS SECTION

- [General Routing | 86](#)

General Routing

- On JRR200, incorrect PEM load percentage for `CLI show chassis power` is observed. [PR1598728](#)

Resolved Issues: 21.2R1

IN THIS SECTION

- [Platform and Infrastructure | 87](#)

Platform and Infrastructure

- On the JRR200 devices, the option-60 (Vendor-Class-Identifier) are not sent during ZTP. [PR1582038](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.2R3 documentation for JRR.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 87](#)

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 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 Juniper Secure Connect

IN THIS SECTION

- [What's New | 89](#)
- [What's Changed | 90](#)
- [Known Limitations | 91](#)
- [Open Issues | 91](#)
- [Resolved Issues | 91](#)
- [Documentation Updates | 92](#)

These release notes accompany Junos OS Release 21.2R3 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 21.2R3 | 90](#)
- [What's New in 21.2R2 | 90](#)
- [What's New in 21.2R1 | 90](#)

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

What's New in 21.2R3

There are no new features or enhancements to existing features for Juniper Secure Connect in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for Juniper Secure Connect in Junos OS Release 21.2R2.

What's New in 21.2R1

There are no new features or enhancements to existing features for Juniper Secure Connect in Junos OS Release 21.2R1.

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 90](#)
- [What's Changed in Release 21.2R2 | 90](#)
- [What's Changed in Release 21.2R1 | 90](#)

Learn about what changed in Junos OS main and maintenance releases for Juniper Secure Connect.

What's Changed in Release 21.2R3

There are no changes in behavior and syntax in Junos OS Releases 21.2R3 for Juniper Secure Connect.

What's Changed in Release 21.2R2

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R2 for Juniper Secure Connect.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for Juniper Secure Connect.

Known Limitations

There are no known limitations in hardware or software in Junos OS Release 21.2R3 for Juniper Secure Connect.

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

Open Issues

There are no known issues in hardware or software in Junos OS Release 21.2R3 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

IN THIS SECTION

- [Resolved Issues: 21.2R3 | 91](#)
- [Resolved Issues: 21.2R2 | 92](#)
- [Resolved Issues: 21.2R1 | 92](#)

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R3

There are no resolved issues in Junos OS Releases 21.2R3 for Juniper Secure Connect.

Resolved Issues: 21.2R2

There are no resolved issues for Juniper Secure Connect in Junos OS Release 21.2R2.

Resolved Issues: 21.2R1

There are no resolved issues for Juniper Secure Connect in Junos OS Release 21.2R1.

Documentation Updates

There are no corrections or changes in Junos OS Release 21.2R3 documentation for Juniper Secure Connect.

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

- [What's New | 93](#)
- [What's Changed | 93](#)
- [Known Limitations | 94](#)
- [Open Issues | 94](#)
- [Resolved Issues | 95](#)
- [Documentation Updates | 95](#)
- [Migration, Upgrade, and Downgrade Instructions | 96](#)

These release notes accompany Junos OS Release 21.2R3 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

IN THIS SECTION

- [What's New in 21.2R3 | 93](#)
- [What's New in 21.2R2 | 93](#)
- [What's New in 21.2R1 | 93](#)

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

What's New in 21.2R3

There are no new features or enhancements to existing features for Junos fusion for enterprise in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for Junos fusion for enterprise in Junos OS Release 21.2R2.

What's New in 21.2R1

There are no new features or enhancements to existing features for Junos fusion for enterprise in Junos OS Release 21.2R1.

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 94](#)
- [What's Changed in Release 21.2R2 | 94](#)
- [What's Changed in Release 21.2R1 | 94](#)

Learn about what changed in the Junos OS main and maintenance releases for Junos fusion for enterprise.

What's Changed in Release 21.2R3

There are no changes in behavior and syntax in Junos OS Releases 21.2R3 for Junos fusion for enterprise.

What's Changed in Release 21.2R2

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R2 for Junos fusion for enterprise.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for Junos fusion for enterprise.

Known Limitations

There are no known limitations in hardware or software in Junos OS Release 21.2R3 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 21.2R3 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: 21.2R3 | 95](#)
- [Resolved Issues: 21.2R2 | 95](#)
- [Resolved Issues: 21.2R1 | 95](#)

Learn which issues were resolved in the Junos OS main and maintenance 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: 21.2R3

- There might be a memory leak observed in Junos Fusion satellite device for the cpd process. [PR1577977](#)
- In rare cases, the anchor logical interface is not created in time which causes a core file to generate during the satellite device provisioning state. [PR1555597](#)

Resolved Issues: 21.2R2

There are no resolved issues in the Junos OS 21.2R2 release for Junos fusion for enterprise.

Resolved Issues: 21.2R1

There are no resolved issues in the Junos OS 21.2R1 release for Junos fusion for enterprise.

Documentation Updates

There are no corrections or changes in Junos OS Release 21.2R3 documentation for Junos Fusion for enterprise.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading Junos OS on an Aggregation Device | 96](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 98](#)
- [Preparing the Switch for Satellite Device Conversion | 99](#)
- [Converting a Satellite Device to a Standalone Switch | 100](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 100](#)
- [Downgrading Junos OS | 101](#)

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 9: EOL and EEOL Releases

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

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

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

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 | 102
- What's Changed | 103
- Known Limitations | 104
- Open Issues | 104
- Resolved Issues | 104
- Documentation Updates | 105
- Migration, Upgrade, and Downgrade Instructions | 105

These release notes accompany Junos OS Release 21.2R3 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

IN THIS SECTION

- What's New in 21.2R3 | 103
- What's New in 21.2R2 | 103
- What's New in 21.2R1 | 103

Learn about new features introduced in the Junos OS main and maintenance releases for Junos Fusion for Provider Edge.

What's New in 21.2R3

There are no new features or enhancements to existing features for Junos fusion for provider edge in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for Junos fusion for provider edge in Junos OS Release 21.2R2.

What's New in 21.2R1

There are no new features or enhancements to existing features for Junos fusion for provider edge in Junos OS Release 21.2R1.

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 103](#)
- [What's Changed in Release 21.2R2 | 103](#)
- [What's Changed in Release 21.2R1 | 104](#)

Learn about what changed in the Junos OS main and maintenance releases for Junos Fusion for provider edge.

What's Changed in Release 21.2R3

There are no changes in behavior and syntax in Junos OS Releases 21.2R3 for Junos fusion for provider edge.

What's Changed in Release 21.2R2

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R2 for Junos fusion for provider edge.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for Junos fusion for provider edge.

Known Limitations

There are no known limitations in hardware or software in Junos OS Release 21.2R3 for Junos fusion for provider edge.

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

Open Issues

There are no known issues in hardware or software in Junos OS Release 21.2R3 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: 21.2R3 | 105](#)
- [Resolved Issues: 21.2R2 | 105](#)
- [Resolved Issues: 21.2R1 | 105](#)

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R3

IN THIS SECTION

- [Junos Fusion Provider Edge | 105](#)

There are no resolved issues in Junos OS Releases 21.2R3 for Junos fusion for provider edge.

Junos Fusion Provider Edge

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

Resolved Issues: 21.2R2

There are no fixed issues in the Junos OS Release 21.2R2 for Junos fusion for provider edge.

Resolved Issues: 21.2R1

There are no fixed issues in the Junos OS Release 21.2R1 for Junos fusion for provider edge.

Documentation Updates

There are no errata or changes in Junos OS Release 21.2R3 documentation for Junos fusion for provider edge.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading an Aggregation Device | 106](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 109](#)
- [Preparing the Switch for Satellite Device Conversion | 109](#)

- [Converting a Satellite Device to a Standalone Device | 111](#)
- [Upgrading an Aggregation Device | 113](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 113](#)
- [Downgrading from Junos OS Release 21.2 | 114](#)

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 21.2R3 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/jinstall64-21.2R3.SPIN-  
domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.2R3.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/jinstall64-21.2R3.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.2R3.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 21.2R3 *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 21.2R3, 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 10: EOL and EEOL Releases

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

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

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

Downgrading from Junos OS Release 21.2

To downgrade from Release 21.2 to another supported release, follow the procedure for upgrading, but replace the 21.2 `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 | 115](#)
- [What's Changed | 134](#)
- [Known Limitations | 142](#)
- [Open Issues | 146](#)
- [Resolved Issues | 163](#)
- [Documentation Updates | 221](#)
- [Migration, Upgrade, and Downgrade Instructions | 222](#)

These release notes accompany Junos OS Release 21.2R3 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 21.2R3 | 116](#)
- [What's New in 21.2R2 | 116](#)

- [What's New in 21.2R1 | 116](#)

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

What's New in 21.2R3

There are no new features or enhancements to existing features for the MX Series routers in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for the MX Series routers in Junos OS Release 21.2R2.

What's New in 21.2R1

IN THIS SECTION

- [Hardware | 117](#)
- [Authentication and Access Control | 118](#)
- [Flow-Based and Packet-Based Processing | 118](#)
- [High Availability | 119](#)
- [Interfaces | 119](#)
- [Juniper Extension Toolkit \(JET\) | 120](#)
- [Junos Telemetry Interface | 121](#)
- [Layer 2 VPN | 122](#)
- [MACsec | 122](#)
- [MPLS | 123](#)
- [Network Address Translation \(NAT\) | 124](#)
- [Network Management and Monitoring | 125](#)
- [Platform and Infrastructure | 126](#)
- [Routing Options | 126](#)
- [Routing Policy and Firewall Filters | 127](#)
- [Routing Protocols | 128](#)

- Services Applications | 129
- Software Defined Networking (SDN) | 131
- Software Installation and Upgrade | 132
- Source Packet Routing in Networking (SPRING) or Segment Routing | 132
- Subscriber Management and Services | 133
- System Management | 134

Learn about new features or enhancements to existing features in this release for the MX Series routers.

Hardware

- The following methods to protect the chassis from excessive current draw and temperature conditions are supported:
 - Configure Junos OS to automatically shut down the PSM, or raise an alarm and log the event when a field-effect transistor (FET) failure is detected in the power supply module (PSM) by using the specified command. [See [thermal-health-check](#)].
 - Configure upgrade of the PSM firmware that will take action when there is an FET failure by using the specified command. [See [request system firmware upgrade](#)].
 - Configure Junos OS to raise an alarm and log events when a PSM with upgraded firmware version shuts down due to an FET failure, Junos OS on the attached device.
 - Configure a monitor to check how much power the chassis draws from the PSM using the specified command. If the system draws more power from the PSM than what it should consume, Junos OS raises an alarm or shuts down the system. [See [watchdog \(PSM\)](#)].
[See [Handling Thermal Health Events Using Thermal Health Check and PSM Watchdog](#)].
- **Support for QSFP-100G-FR transceivers (MX2010 and MX2020 with MPC9E and MIC-MRATE)**—Starting in Junos OS Release 21.2R1, the MX2010 and MX2020 routers with the MPC9E+MIC-MRATE support the QSFP-100G-FR transceivers.
[See [Hardware Compatibility Tool](#).]
- **Support for QSFP-100G-LR transceivers (MX2010 and MX2020 with MPC9E and MIC-MRATE)**—Starting in Junos OS Release 21.2R1, the MX2010 and MX2020 routers with the MPC9E+MIC-MRATE support the QSFP-100G-LR transceivers.
[See [Hardware Compatibility Tool](#).]

- **Support for QSFP-100G-FR transceivers (MX2010 and MX2020 with MX2K-MPC9E and MIC-MACSEC-MRATE)**—Starting in Junos OS Release 21.2R1, the MX2010 and MX2020 routers with the MPC9E+MIC-MACSEC-MRATE support the QSFP-100G-FR transceivers.

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

- **Support for QSFP-100G-LR transceivers (MX2010 and MX2020 with MPC9E and MIC-MACSEC-MRATE)**—Starting in Junos OS Release 21.2R1, the MX2010 and MX2020 routers with the MPC9E+MIC-MACSEC-MRATE support the QSFP-100G-LR transceivers.

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

- **Support for the JNP-SFP-10G-BX10D and JNP-SFP-10G-BX10U transceivers (MX10003)**—Starting in Junos OS Release 21.2R1, the MX10003 routers support the JNP-SFP-10G-BX10D and JNP-SFP-10G-BX10U transceivers.

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

- **Support for QSFP-100G-LR transceivers (MX240, MX480, and MX960 with MPC7E-MRATE)**—Starting in Junos OS Release 21.2R1, the MX240, MX480, and MX960 routers with the MPC7E-MRATE support the QSFP-100G-LR transceivers.

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

- **Support for QSFP-100G-FR transceivers (MX240, MX480, and MX960 with MPC7E-MRATE)**—Starting in Junos OS Release 21.2R1, the MX240, MX480, and MX960 routers with the MPC7E-MRATE support the QSFP-100G-FR transceivers.

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

Authentication and Access Control

- **802.1X authentication on trunk ports (MX Series)**—Starting with Junos OS Release 21.2R1, you can enable 802.1X authentication on trunk ports. We support authentication on the trunk port only in single supplicant and single-secure supplicant modes.

[See [802.1X Authentication on Trunk Ports](#).]

Flow-Based and Packet-Based Processing

- **Carrier-grade NAT (CGNAT) J-Flow logging (MX240, MX480, and MX960 with MX-SPC3 card)**—Starting in Junos OS Release 21.2R1, we've enhanced NAT logging using J-Flow version 9 and IPFIX format to generate logs. While creating or deleting events in NAT44 or NAT64 sessions, jflow-logs are generated.

[See [Understanding NAT Event Logging in Flow Monitoring Format on an MX Series Router or NFX250](#).]

High Availability

- **Unified ISSU with enhanced mode support (MX2008, MX2010, and MX2020 with MPC11E)**—Starting in Junos OS Release 21.2R1, we support unified in-service software upgrade (ISSU) in enhanced mode. Enhanced mode runs a second copy of the Junos OS software in standby mode. The second copy is ready to take over when the software updates the old image to a new one. Enhanced mode reduces packet loss to near-zero during the ISSU process.

Use the `request system software validate in-service-upgrade package-name.tgz enhanced-mode` command to verify that your device and the target release are compatible with enhanced mode. Use the `request system software in-service-upgrade package-name.tgz enhanced-mode` command to use unified ISSU with enhanced mode.

[See [How to Use Unified ISSU with Enhanced Mode.](#)]

- **NSR support for RSVP-TE dynamic tunnels (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support nonstop active routing (NSR) for RSVP-Traffic Engineering (RSVP-TE) dynamic tunnels.

[See [Nonstop Active Routing Concepts.](#)]

- **Distributed and Inline BFD support for IPv6 link-local address (MX240, MX480, and MX960)**—Starting in Junos OS 21.2R1, we support distribution of OSPFv3 and ISIS BFD sessions which use IPv6 link local address. To forward packets with link local ipv6 address as destination from micro-kernel, we provide next-hop id as part of the packet which the PFE uses to forward the packet on right interface. Also, we support inline mode and by default the IPv6 Link local BFD sessions will operate in inline mode. This feature is supported on MX Series MPCs 1 to 9. This is not supported on MX Series MPCs 10 and 11.

[See [Understanding Distributed BFD.](#)]

Interfaces

- **Support for VLAN rewrite operations on CCC interfaces (MX480 and MX960)**—Starting in Junos OS Release 21.2R1, you can configure VLAN rewrite operations on CCC interfaces.

[See [Configuring Q-in-Q Tunneling and VLAN Q-in-Q Tunneling and VLAN Translation.](#)]

- **Support for coexistence of source IP hash with consistent hash (MX Series)**—Starting in Junos OS Release 21.2R1, source IP hash, which allows the flow from a particular source IP to always be hashed to the same link while load-balancing the flows across multiple paths, supports consistent hash, which prevents the reordering of flows to active paths in an ECMP group when one or more paths fail.

NOTE: This feature is applicable only to external BGP (EBGP) ECMP paths.

[See [Configuring Load Balancing Using Source or Destination IP Only](#) and [Configuring Consistent Load Balancing for ECMP Groups](#).]

- **AMS on MPC10E line card (MX240, MX480, and MX960 with MX-SPC3)**—Starting in Junos OS Release 21.2R1, we support load balancing and high availability (HA) features on aggregated multiservices (AMS) interfaces for Layer 4 and Layer 7 services such as stateful firewall, intrusion detection service (IDS), and the Traffic Load Balancer (TLB) application.

Juniper Extension Toolkit (JET)

- **JET API support for GRE tunneling (MX204, MX240, MX480, MX960, MX2010, MX2020, and MX10003 with MPC1-MPC9E, MPC10E, or MPC11E; and VMX)**—Starting in Junos OS Release 21.2R1, we have enhanced Juniper Extension Toolkit (JET) APIs to support GRE tunneling and packet translation between IPv6 and IPv4. With the RIB (also known as routing table) service API and flexible tunnel profile API, you can embed GRE encapsulation and translation profiles. With the flexible tunnel service API, you can embed GRE de-encapsulation profiles.

[See [JET APIs on Juniper EngNet](#).]

- **BGP route service API supports programming routes with IP-IP encapsulation attributes (MX240, MX480, MX960, PTX1000, QFX5110, QFX5200, QFX10002, and QFX10008)**—Starting in Junos OS Release 21.2R1, you can use the BGP route service API to program BGP routes with IP over IP (IP-IP) encapsulation attributes. You can specify the tunnel type, the remote endpoint address, and the color of the route. Keep the following in mind:
 - The egress endpoint must be a unicast IPv4 address.
 - The colors encoded in `tunnel_encap` and `extended_community` must match.
 - If the encapsulation `ext_com` and the tunnel attribute are both present, the egress endpoint must match the next-hop address.

To enable this feature, configure the `bgp-signal` option at the `[edit routing-options dynamic-tunnels tunnel-name]` hierarchy level. The rest of your dynamic tunnel CLI configuration does affect the functionality of the programmed tunnels.

[See [dynamic-tunnels](#) and [JET APIs on Juniper EngNet](#).]

Junos Telemetry Interface

NOTE: For Routing Engine telemetry sensors supported by this platform, see [Telemetry Sensor Explorer](#). If any Platform Forwarding Engine sensors have been added for this release, they are listed below

- **End-of-message notification for Routing Engine sensors (EX2300, EX4300, EX4300-MP, EX9200, MX240, MX960, MX10016, MX2010, MX2020, PTX1000, PTX3000, PTX10001, QFX5100, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we've introduced an end-of-message (EoM) Boolean flag for all Junos telemetry interface (JTI) Routing Engine sensors. The flag notifies the collector that the current wrap has completed for a particular sensor path. A wrap is a complete key-value data dump for all the leaves under a sensor path.

The EoM flag also enables the collector to detect when the end of wrap occurs without having to compare stream creation timestamp values that the collector receives from the packets. Comparing timestamp values is costly time-wise and delays data aggregation.

To use this feature with gRPC Network Management Interface (gNMI) transport or Remote Procedure Call (gRPC), retrieve the protobuf files from the relevant branch on the [Juniper Networks](#) download site:

- GnmJuniperTelemetryHeaderExtension.proto (gNMI)
- agent.proto (for gRPC)

For example: <https://github.com/Juniper/telemetry/blob/master/20.3/20.3R1/protos/GnmJuniperTelemetryHeaderExtension.proto>.

After you download and install the new protobuf files on a collector, the EoM field is present in the packets received.

[See [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **CoS sensor support (MX204, MX240, MX960, MX2010, MX2020, MX10003, MX10008, MX10016, MX-ELM and vMX)**

Starting in Junos OS Release 21.2R1, we support the following streaming sensors with Junos telemetry interface (JTI).

- Interface queue extended statistics Packet Forwarding Engine sensors supported with Remote Procedure Call (gRPC): `/interfaces/interface/state/counters/out-queue/lp-red-drop-pkts`, `/interfaces/interface/state/counters/out-queue/hp-red-drop-pkts`, `/interfaces/interface/state/counters/out-queue/queued-pkts`, and `/interfaces/interface/state/counters/out-queue/queued-bytes`.

- CoS interface set description Routing Engine sensor supported with gRPC: `/qos/interfaces/interface/state/interface-id`.
- Forwarding class to queue mapping Routing Engine sensors supported with gRPC: `/qos/forwarding-groups/forwarding-group/state/name` and `/qos/forwarding-groups/forwarding-group/state/output-queue`.
- Interface extended statistics sensor with native (UDP) support: `/junos/system/linecard/interface/queue/extended-stats/`.

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

- **JTI: logical interface statistics for IPv4 and IPv6 family input and output counters (MX Series and PTX Series routers using third-generation FPCs)**—Starting in Junos OS Release 21.2R1, you can stream per-family logical interface statistics for IPv4 and IPv6 traffic using Junos telemetry interface (JTI) and Remote Procedure Calls (gRPC) to an outside collector.

To access these sensors, use the resource paths `/junos/system/linecard/interface/logical/family/ipv4/usage/` and `/junos/system/linecard/interface/logical/family/ipv6/usage/` in a subscription.

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

Layer 2 VPN

- **Support for Layer 2 services on SR-TE tunnels using transport class (MX series, PTX Series, and vMX)**—Starting in Junos OS Release 21.2R1, you can configure the following Layer 2 services on colored and non-colored segment routing traffic engineer (SR-TE) tunnels using transport classes.
 - Layer 2 Circuits
 - Layer 2 VPN
 - BGP VPLS

[See [Layer 2 Circuit Overview](#), [Introduction to Configuring Layer 2 VPNs](#), and [BGP Classful Transport Planes Overview](#) .]

MACsec

- **MACsec with GRES and NSR (MX140 and MX480 with the MIC-3D-20GE-SFP-E, MIC-3D-20GE-SFP-EH, and MIC-MACSEC-20GE line cards)**—Starting in Junos OS Release 21.2R1, Media Access Control Security (MACsec) support includes GRES and nonstop active routing (NSR) to provide nonstop MACsec service during a Routing Engine switchover.

[See [Configuring Media Access Control Security \(MACsec\) on Routers](#).]

MPLS

- **Support for the EVPN-LAN and P2P services using an MPLS-based core with IPv6 underlay (MX Series)**—Starting in Junos OS Release 21.2R1, we extend support for the EVPN-VXLAN and point-to-point (P2P) services using an MPLS-based IPv6 underlay. The services operate over an MPLS-based core with IPv6 addresses on the PE routers using Segment Routing with Multiprotocol Label Switching (SR-MPLS). The services also operate on the segment routing-traffic engineering (SR-TE) addresses that are responsible for the path calculation between the EVPN PE devices. You can use the EVPN-MPLS commands with the MPLS-based IPv6 underlays.

To enable EVPN-MPLS-over-IPv6 functionality, set the protocols `evpn encapsulation mpls-inet6` configuration statement for each EVPN routing-instance in the `[routing-instances <routing-instance-name> protocols evpn encapsulation]` hierarchy level.

[See [Understanding EVPN with VXLAN Data Plane Encapsulation](#) and `protocols evpn encapsulation mpls-inet6`.]

- **RSVP signaling over IS-IS nonforwarding adjacency (MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, you can configure any Level 1-Level 2 (L1-L2) routers that have been configured as a flood-reflector client to expand the flood-reflector hops in the Explicit Route Objects (EROs) carried in the Path messages. This feature enables the L1-L2 routers to signal RSVP over IS-IS nonforwarding adjacency by expanding the flood-reflector hops in the EROs instead of propagating the Path messages over the UDP tunnels.

To know how to configure the flood-reflector interfaces, see [How to Configure Flood-Reflector Interfaces in IS-IS Networks](#).

To expand the flood-reflector hops in EROs, use the `rsvp expand-flood-reflector-hop` configuration statement at the `[edit protocols]` hierarchy level.

Using the `traceoptions (Protocols RSVP)` command with the `flag event` option, you can view the new trace messages in the file that is created.

The `show ted database` and `show rsvp session` command outputs introduce the following additional information:

Command	New Output Field	Description
<code>show ted database</code>	Flood reflector client, cluster-id <i><number></i>	Displays flood-reflector related information on the TE links and the cluster ID that the you have connected at the client side.

(Continued)

Command	New Output Field	Description
	Flood reflector, cluster-id <number>	Displays flood-reflector related information on the TE links and the cluster ID that you have connected in the flood reflector.
show rsvp session	Explct hop <ip-address> expanded	Displays the specific hop in the EROs that has been expanded by the router.

[See [How to Configure Flood-Reflector Interfaces in IS-IS Networks](#), [show ted database](#), [show rsvp session](#), and [traceoptions \(Protocols RSVP\)](#).]

- **RSVP-TE supports preempting secondary LSPs that are signaled but not active (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, you can preempt secondary LSPs that are signaled but not active and configure the hold priority of the secondary standby label-switched path (LSP) for RSVP-Traffic Engineering (RSVP-TE). This helps to bring up non-standby secondary path LSPs with higher setup priority which are not able to come-up because of bandwidth crunch. To configure the non-active hold priority value for a secondary standby path, use the `non-active-hold-priority` statement at the `[edit protocols mpls label-switched-path <isp-name> secondary <path-name>]` hierarchy level. You can set the priority from 0 through 7, where 0 is the highest priority and 7 is the lowest.
- **Support for 128 primary paths per static segment routing LSP (MX Series and PTX Series)**—Starting in Junos OS 21.2R1, we've increased the maximum number of segment-list bindings to an LSP tunnel from 8 to 128, with not more than 1000 tunnels per system. A maximum of 128 primary paths are supported per static segment routing LSP.

[See [Static Segment Routing LSP Limitations](#).]

Network Address Translation (NAT)

- **IPv6 MTU for NAT64 and NAT464 traffic (MX240, MX480, and MX960 with the MX-SPC3 card)**—Starting in Junos OS Release 21.2R1, you can configure IPv6 MTU for NAT64 and NAT464 traffic using the `ipv6-mtu` option at the `[service-set nat-options]` hierarchy level.

[See [Stateful NAT64 Overview](#).]

Network Management and Monitoring

- **CFM CCM support on PS interfaces (MPC7E, MPC8E, MPC9E, MPC10E, and MPC11E line cards)**—Starting in Junos OS Release 21.2R1, we support connectivity fault management (CFM) continuity check messages (CCM) on PS interface part of EVPN. You can configure:
 - CCM for down maintenance association end points (MEPs), that are down, on the PS interface to monitor the Ethernet networks for connectivity faults.
 - Remote defect indication (RDI) for the CCM frame.
 - Action profile with action link down for the remote MEP to bring down the PS interface when connectivity is lost.
 - Ethernet link trace (ETH-LT) and loopback (ETH-LB) are supported on the CFM session.

[See [Ethernet OAM Connectivity Fault Management](#).]

- **OAM ping support for segment routing with IPv6 (SRv6) network programming (MX Series)**—Starting in Junos OS Release 21.2R1, you can perform the Operation, Administration, and Maintenance (OAM) ping operation for any SRv6 segment identifier (SID) whose behavior allows upper layer header processing for an applicable OAM payload.

Because segment routing with IPv6 data plane (SRv6) adds only the new type-4 routing extension header, you can use the existing ICMPv6-based ping mechanisms for an SRv6 network to provide OAM support for SRv6. Ping with O-Flag (segment header) is not supported.

[See [ITU-T Y.1731 Ethernet Service OAM Overview](#) and [How to Enable SRv6 Network Programming in IS-IS Networks](#).]

- **Support for syslog over TLS (EX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, you can transport syslog (control plane) over Transport Layer Security (TLS) protocol. Encapsulating syslog over 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
- 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.

- **Syslog support to replay events (MX Series)**—Starting in Junos OS Release 21.2R1, you can replay syslog events over gRPC. Configure the last `minute` statement at the `[edit system syslog grpc-replay]` hierarchy level to replay events. You can also filter events based on facility and priority. Use the `facility` statement to filter events according to facility, and use the `priority` statement to filter events according to the priority at the `[edit system syslog grpc-replay]` hierarchy level. You can use the `facility` and the `priority` options to filter replay or live events.

[See [grpc-replay](#).]

Platform and Infrastructure

- **New MX10K-LC480 line card (MX10008 and MX10016)** —Starting in Junos OS Release 21.2R1, we've a new MX10K-LC480 line card with 48 SFP/SFP+ ports. The MX10K-LC480 has two Packet Forwarding Engines, each providing a maximum bandwidth of up to 240 Gbps.

You can configure the ports as 10-Gigabit Ethernet interfaces or 1-Gigabit Ethernet interfaces. By default, the ports are 10-Gigabit Ethernet interfaces.

NOTE: You must install the MX10K-LC480 line card in the MX10008 and MX10016 routers along with the front panel with filter.

You can configure the speed at the PIC level or port level. Configure the port speed of the line card at the `[[set chassis fpc <fpc> pic <number> pic-mode <mode>]]` or `[[set chassis fpc <fpc> pic <number> port <number>]]` hierarchy.

Benefits of MX10K-LC480 Line card

- Low cost card
- Interoperability with the existing JNP10K-LC1201 card

For information about the software features support, see [Protocols and Applications Supported by MX10K-LC480 for MX Series Routers](#).

Routing Options

- **Enhancements to prefix-limit and accepted-prefix-limit configuration statements, and updates to show bgp neighbor command (ACX1000, EX9200, MX Series, PTX5000, and QFX10002)**— Starting from Junos OS Release 21.2R1, the `prefix-limit` and `accepted-prefix-limit` configuration statements include the following options:

- **drop-excess <percentage>**—If you include the drop-excess <percentage> option, the excess routes are dropped when the maximum number of prefixes is reached. If you specify a percentage, the routes are logged when the number of prefixes exceeds that percentage value of the maximum number.
- **hide-excess <percentage>**—If you include the hide-excess <percentage> option, the excess routes are hidden when the maximum number of prefixes is reached. If you specify a percentage, the routes are logged when the number of prefixes exceeds that percentage value of the maximum number.

The show `bgp neighbor` command has been enhanced to display the following additional information:

- Count of prefixes that are dropped or hidden based on network layer reachability information (NLRI) when the maximum allowed prefixes threshold is exceeded.
- Alerts when a peer starts to drop or hide routes.
- Configuration details of the `prefix-limit` and `accepted-prefix-limit` configuration statements.

[See [prefix-limit](#), [accepted-prefix-limit](#), [show bgp neighbor](#), and [Multiprotocol BGP](#).]

- **Forwarding class counters support for flat-file-profile (MX Series and vMX)**—Starting in Junos OS Release 21.2R1, the flat-file-profile statement supports forwarding class counters. You can now switch from the ingress CoS queue counters configuration to the forwarding class counters configuration. To enable the forwarding class counters feature, configure the `use-fc-ingress-stats` statement at the `[edit accounting-options flat-file-profile profile-name]` hierarchy level.

[See [flat-file-profile \(Accounting Options\)](#).]

Routing Policy and Firewall Filters

- **Enhanced firewall filter processing on MPC10E and MPC11E line cards (MX Series)**—Starting in Junos OS Release 21.2R1, MX Series routers evaluate the terms attached to a firewall filter in an optimized fashion, and the maximum number of terms per filter increases to 8000.

[See [Understanding Firewall Filter Match Conditions](#).]

- **TCP SYN cookie (MX480 and MX960 with SPC3 card)**—Starting in Junos OS Release 21.2R1, we support the TCP SYN cookie. You can configure `syn-cookie` for the TCP protocol for source and destination.

[See [Configuring Network Attack Protection With IDS Screens for Next Gen Services](#).]

Routing Protocols

- **Support for origin validation with BGP sharding (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, you can use origin validation with BGP sharding. You can configure rib-sharding with routing-options validation.
- **BMP with BGP sharding and update I/O (JRR Series, MX Series, PTX Series, and vMX)**—Starting in Junos OS Release 21.2R1, we support BGP Monitoring Protocol (BMP) with BGP sharding and update I/O in the multithreaded mode.
- **Basic MVPN support with BGP sharding (cRPD, JRR200, MX2020, PTX5000, and QFX10002)**—Starting in Junos OS 21.2R1, we support the basic multicast virtual private network (MVPN) functionalities with BGP sharding.

NOTE: Sharding is not supported for the MVPN address family.

- **Support for BGP SR-TE policy advertisement and error handling (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, if the SDN controller cannot directly install SR-TE routes on non-Juniper Networks devices, the controller installs the BGP SR-TE policy on the route reflector, which forwards the SR-TE routes to non-Juniper devices.

To advertise SR-TE policy to non-Juniper devices, define a BGP policy that includes the family inet-srte statement at the [edit policy-options policy-statement term from protocol bgp] hierarchy level.

To push an unlabeled IP packet before other labels, include the inet-color-append-explicit-nullstatement at the [edit protocols source-packet-routing] hierarchy level.

- **Support for SRv6 network programming and Layer 3 Services over SRv6 in BGP (MX Series)**—Starting in Junos OS Release 21.2R1, you can configure BGP based Layer 3 service over SRv6 core. You can enable Layer 3 overlay services with BGP as control plane and SRv6 as dataplane. SRv6 network programming provides flexibility to leverage segment routing without deploying MPLS. Such networks depend only on the IPv6 headers and header extensions for transmitting data.

To configure IPv4 VPN and IPv6 VPN service over SRv6 core, include the end-dt4-sid sid and the end-dt6-sid sid statements at the [edit routing-instances routing-instance name protocols bgp source-packet-routing srv6 locator name] hierarchy level.

[See [Understanding SRv6 Network Programming and Layer 3 Services over SRv6 in BGP.](#)]

- **Support for BGP classful transport (CT) with underlying colored SRTE tunnels (MX Series and PTX Series with FPC-PTX-P1-A)**— Starting in Junos OS Release 21.2R1, BGP-CT can resolve service routes using the transport RIBs and compute the next-hop. Services currently supported over BGP-CT can also use the underlying SRTE colored tunnels for route resolution.

To enable BGP CT service route resolution over underlying SRTE colored tunnels, include the `use-transport-class` statement at the `[edit protocols source-packet-routing]` hierarchy level.

[See [use-transport-class](#).]

- **Flexible algorithm inter-level leaking support for SRv6 and SR-MPLS in ISIS (ACX Series, MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support flexible algorithm inter-level leaking for SRv6 and SR-MPLS in IS-IS. Also, we partially support TE-App RFC 8919 in its basic form and extends 6PE support for flexible algorithm.

Services Applications

- **Support for the Juniper Resiliency Interface (MX480, MX960, MX2010, MX2020 and vMX)**—Starting in Junos OS Release 21.2R1, you can use our new Juniper Resiliency Interface (JRI) to detect, correlate, and mitigate exceptions. JRI extends the inline monitoring services feature with Juniper-specific IPFIX information elements (IEs) for exception data and introduces the concept of an Observation Cloud, which is a set of Observation Domains. You can send the IPFIX packets to either an on-box or an off-box collector.
 - You configure JRI with the `exceptions`, `store`, and `tracoptions` statements at the `[edit system resiliency]` hierarchy level.
 - You configure which categories of PFE exceptions are reported to a particular inline-monitoring instance with the `exception-reporting inline-monitoring-instance instance-name category category-name` statement at the `[edit chassis fpc name pfe name]` hierarchy level.
 - You configure the Juniper-specific IEs with the `primary-data-record-fields` statement at the `[edit services inline-monitoring templates template-name]` hierarchy level.
 - You configure the Observation Cloud ID with the `observation-cloud-id` statement at the `[edit services inline-monitoring]` hierarchy level.

[See [Inline Monitoring Services Configuration](#).]

- **Support for Routing-Engine based traffic sampling (MX Series with MPC10E and MPC11E line cards)**—Starting in Junos OS Release 21.2R1, you can configure Routing-Engine based traffic sampling. Traffic sampling enables you to copy traffic to a line card that performs flow accounting while the router forwards the packet to its original destination. You configure either an input or output firewall filter with a matching term that contains the `then sample` statement. Routing-Engine based traffic sampling supports only the version 5 and version 8 formats for exporting flow records.

[See [Configuring Traffic Sampling on MX, M and T Series Routers](#).]

- **Support for translation and GRE tunneling in data center environment (MX Series Routers)**—Starting in Junos OS Release 21.2R1, as part of upgrading the customer network for PaaS services, we

support enhancement to your enterprise edge routers (MX routers). You can configure your edge routers to enable translation (IPv4 to IPv6 and IPv6 to IPv4) and GRE tunneling of the translated packets through the Juniper Extension Toolkit (JET) APIs. The edge routers now provide access to a Private Link Service offered as Platform as a Service (PaaS), bypassing the data center gateways.

[See [show flexible-tunnels profile](#) and [show-route](#) .]

- **Support for any firewall filter family and Layer 2 firewall filter families for inline monitoring services (MX Series with MPC10E and MPC11E line cards)**—Starting in Junos OS Release 21.2R1, you can configure the any, bridge, ccc, or vpls family firewall filter with the term action `inline-monitoring-instance` *inline-monitoring-instance-name*.

[See [Inline Monitoring Services Configuration](#).]

- **Support for inline NAT services (MX240, MX480, MX960, MX2010, and MX2020 with MPC10E and MX2K-MPC11E line cards)**—Starting with Junos OS Release 21.2R1, we support inline NAT services. We support the following features:

- 1:1 static address mapping
- Bidirectional mapping: source NAT for outbound traffic and destination NAT for inbound traffic
- No limit on number of flows
- Source, destination, and twice NAT
- Source NAT44
- Destination NAT44
- Source NAT with Interface Style
- Destination NAT with Interface Style
- Inline NAT with VRF

[See [Inline NAT](#).]

- **Interoperability of MPC10E with MX-SPC3 for IPSec services steering (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.2R1, the MPC10E-15C-MRATE and MPC10E-10C-MRATE interoperates with the MX-SPC3 card to enable the packet forwarding path that steers packets to the MX- SPC3 card. The MPC10E line card can perform the ingress or the egress processing for IPSec services packets through the `st0` and `vms` interfaces, nexthops, and the routes programmed in the line card.

[See [MPC10E-15C-MRATE](#) and [MPC10E-10C-MRATE](#).]

- **Interoperability of MPC10E with MX-SPC3 to support TLB (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.2R1, the MPC10E-15C-MRATE and the MPC10E-10C-MRATE interoperates

with the MX-SPC3 card to support traffic load balancing. Using the Traffic Load Balancer (TLB) application, you can distribute traffic among multiple servers in a server group and perform health checks to determine whether any servers should not receive traffic. TLB supports multiple VPN routing and forwarding instance (VRF) instances..

[See [Traffic Load Balancer Overview](#).]

- **Support for unidirectional session refreshing (MX Series routers with MS-MPCs and MX-SPC3 services card)**—Starting in Junos OS Release 21.2R1, we support unidirectional session refreshing.

For a service set, you can configure unidirectional session refreshing for the in-zone and the out-zone.

At the [edit services service-set <service-set-name> service-set-options] hierarchy level, you can enable unidirectional session forwarding for:

- Input (in-zone), by configuring the statement unidirectional-session-refreshing input.
- Output (out-zone), by configuring the statement unidirectional-session-refreshing output

[See [service-set-options](#).]

Software Defined Networking (SDN)

- **SLCs support new asymmetric profile, multiversion software interoperability, GRES, and fabric hardening (MX2010 and MX2020 with MX2K-MPC11E)**—Starting in Junos OS Release 21.2R1, Junos node slicing with sub line cards (SLCs) supports the following features:

- A new asymmetric profile which supports assigning DRAM size of 9 GB or 17 GB to an SLC independent of the PFE subset assignments.
- Multiversion Software Interoperability

NOTE: If you are using sub line cards, Junos OS node slicing in 21.2R1 is not multiversion interoperable with any earlier release of Junos OS, including 21.1R1. For a GNF in a node-sliced system that uses SLCs to run Junos OS 21.2R1, all other GNFs and BSYS on that system must also run 21.2R1.

- Fabric hardening
- GRES on BSYS and guest network functions (GNFs). SLCs also support handling failure of links between the server and Control Boards (CBs).

The SLC feature enables you to configure logical partitions of the MPC11E line card and assign each partition to different guest network functions (GNFs) in an external server-based Junos node slicing setup.

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

Software Installation and Upgrade

- **Increased memory allocation for Junos VM (MX204)**—Starting in Junos OS Release 21.2R1, we support increased memory allocation for Junos VM. The available VM size options are default (16GB) and high (24GB). After you update the VM size, you must perform a system reboot using the `request vmhost reboot` statement.

Before you increase the memory, please contact Juniper Networks technical support to know the use cases that we support. After the memory upgrade, if you want to downgrade the Junos OS image, revert the VM memory to default and perform a system reboot using the `request vmhost reboot` command.

[See [VM Host Overview.](#)]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Static route resolution over SR-TE tunnel (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support static route resolution over segment routing-traffic engineered (SR-TE) colored and uncolored label-switched paths (LSPs). To enable this feature, configure the `spring-te-lsp-next-hop` statement at the `[edit routing-options static destination]` and `[edit routing-options rib rib name static destination]` hierarchy levels. The feature support extends towards static, DTM, BGP-SR-TE, and PCEP source types that are currently supported by Source Packet Routing in Networking-Traffic Engineering (SPRING-TE). If a source is not configured, by default, it takes the next hop as static.

You must configure the `tunnel-tracking` statement at the `[edit protocols source-packet-routing]` hierarchy level to enable this feature. This feature enhances the accuracy of first-hop label-based tunnel status for SR-TE tunnels according to their route resolution.

[See [spring-te-lsp-next-hop](#) and [source-packet-routing](#).]

- **Express segments using SR-TE underlay (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we've introduced SR-TE underlay path support for express segments to enable end-to-end transport of segment routing-traffic engineered (SR-TE) label-switched paths (LSPs) for very large multi-domain networks. The path is automated using `segment-set` or `template` policies for uncolored or colored segment routing policies. The `rib-group` configuration is required to import addresses to `inet.3` for colored segment routing policies. When the express segments underlay is colored SR-TE, you need to configure the `no-chained-composite-next-hop` statement at the `[edit protocols source-packet-routing]` hierarchy level for the express segment to install the correct flattened next hop.

This feature has the following limitations:

- When the express segments underlay is colored SR-TE, the express segment does not inherit the SR-TE LSP underlay attributes (SR-TE name, metric).
- The `install-nexthop` option at the `[edit policy-options policy-statement policy-name term term-name then]` hierarchy level to filter a specific SR-TE LSP by its name is not supported.
- Express segments do not consider the respective weights of the primary and secondary segment lists of SR-TE LSP. Secondary LSP segments can be preferred for traffic even when the primary segment is up.

[See [Express Segment LSP Configuration](#).]

Subscriber Management and Services

- **Advanced services support for static subscribers (MX240, MX480, and MX960 with MS-MPCs)**—Starting in Junos OS Release 21.2R1, you can configure the `static-subscriber-application` statement at the `[edit services service-set-name service-set-options]` hierarchy level to attach advanced services, such as deep packet inspection (DPI), to the static subscriber. [See [Configuring Subscriber-Aware and Application-Aware Traffic Treatment Overview](#) and [service-set \(Subscriber-Aware\)](#).]
- **Support for Broadband Edge subscriber management and services (MX10008 and MX10016 with MX10K-LC2101 and MX10K-LC480)**—Starting in Junos OS Release 21.2R1, we support subscriber management and services. The line cards also support subscriber access, subscriber authentication, service activation, and deactivation.

[See [Subscriber Management Overview](#).]

- **Junos Multi-Access User Plane support for 5G user plane function (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 21.2R1, Junos Multi-Access User Plane supports routers functioning as user plane functions (UPFs) in accordance with 3GPP Release 15 CUPS architecture. This provides high-throughput 5G fixed and mobile wireless service in non-standalone (NSA) mode. This includes support for the following:
 - N3, N4, N6, and N9 interface support
 - Roaming through the N9 interface
 - GPRS tunneling protocol, user plane (GTP-U) tunneling to the control plane
 - QoS Flow ID (QFI) support for 5G QoS flows

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

- **Support for PWHT with VC type 11 (MX Series routers with MPC7E, MPC10E, MPC9E, or MPC11E line cards)**—Starting in Junos OS Release 21.2R1, you can configure a pseudowire headend

termination (PWHT) interface on a service PE router with ethernet-tcc encapsulation on the interface. With this feature, the service PE router does not have to support TDM/SONET/SDH-encapsulated traffic coming from access-side customers. The IP-based point-to-point pseudowire—which is an LDP-signaled FEC 128 (virtual circuit (VC) type 11)—connects the service PE router to the access device that is connected to the access CE router.

You configure the pseudowire to terminate into a Layer 3 VPN instance or a global IP table. The service PE router uses ARP mediation to resolve Layer 2 addresses when different resolution protocols are used on either end of a circuit.

The feature supports IPv4 and IPv6 payloads, and unicast and multicast traffic.

[See [Configuring a PWHT with VC 11 Type Support.](#)]

System Management

- **Support for PTP over Ethernet and hybrid mode over LAG interfaces (MX240, MX480, and MX960)**
—The MPC2E NG and MPC3E NG line cards support Precision Time Protocol (PTP) over Ethernet and hybrid mode over a link aggregation group (LAG).

Limitations

There could be some performance limitations during a switchover from the active line card to the secondary line card and vice versa in a multi-line card scenario because of hardware limitations.

If an unsupported line card is configured as the primary or secondary interface, the configuration goes through, but an error message is displayed in the output of the show ptp slave/primary CLI command. You must configure only supported line cards (MPC5E and MPC6E) to avoid this issue.

[See [Understanding Hybrid Mode](#) and [Precision Time Protocol Overview.](#)]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3](#) | 135
- [What's Changed in Release 21.2R2](#) | 137
- [What's Changed in Release 21.2R1](#) | 137

Learn about what changed in the Junos OS main and maintenance releases for MX Series routers.

What's Changed in Release 21.2R3

IN THIS SECTION

- [General Routing | 135](#)
- [Interfaces and Chassis | 135](#)
- [Layer 2 Ethernet Services | 135](#)
- [Network Management and Monitoring | 136](#)
- [Routing Protocols | 136](#)

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 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.

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.

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 the `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

- **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](#).]

- **Changes to the NETCONF `<edit-config>` RPC response (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<edit-config>` operation returns an error, the NETCONF server does not emit a `<load-error-count>` element in the RPC response. In earlier releases, the `<edit-config>` RPC response includes the `<load-error-count>` element when the operation fails.

Routing Protocols

- To achieve consistency among resource paths, the resource path `/mpls/signalling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter ip-addr='address'/state/counters name='name'/out-pkts/` is changed to `/mpls/signaling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter ip-addr='address'/state/counters name='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 21.2R2

IN THIS SECTION

- [General Routing | 137](#)

General Routing

- **Support for multiple proxy-id list (MX5, MX10, MX40, MX80, MX104, MX240, MX480, MX960, MX2008, MX2010, and MX2020)**—MX Series routers do 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))

What's Changed in Release 21.2R1

IN THIS SECTION

- [Class of Service \(CoS\) | 138](#)
- [EVPN | 138](#)
- [General Routing | 138](#)
- [High Availability | 139](#)
- [Interfaces and Chassis | 139](#)
- [Junos XML API and Scripting | 140](#)
- [Layer 2 Ethernet Services | 140](#)
- [Layer 2 Features | 140](#)
- [Network Management and Monitoring | 141](#)
- [Software Defined Networking \(SDN\) | 142](#)
- [VPNs | 142](#)

Class of Service (CoS)

- Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

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.
- **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.

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**—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.](#)]

- **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.
- **VLAN isolation disabled by default (MX480, MX960, MX2008, MX2010, and MX2020)**—For Junos node slicing, the internal control plane no longer isolates GNFs from each other by default. The internal network has sufficient bandwidth to accommodate GNFs without needing to isolate GNFs from each other. However, if you want to isolate the internal traffic of each GNF from all others, you must configure the `set chassis network-slices vlan-isolation` CLI configuration statement (which is

applicable for all uses except with sub line cards) on all the Routing Engines of the BSYS and GNFs and then reboot the chassis. If you want to configure the sub line card feature, you must ensure that VLAN isolation is disabled. We have deprecated the configuration statement `no-vlan-isolation`.

[See [vlan-isolation](#).]

- **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.

High Availability

- **Inline Mode for IPv6 Link local BFD sessions (MX240, MX480, and MX960)**—Starting in Junos OS 21.2R1, if an IPv6 link-local BFD session is set up, the transmission and reception entries are distributed and by default operates in inline mode. Prior to Junos OS 21.2R1 release, the transmission and reception were handled by the Routing Engine.

Interfaces and Chassis

- **Blocking duplicate IP detection in the same routing instance (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, and SRX Series)**—Junos will no longer accept duplicate IPs between different logical interfaces in the same routing instance. Refer to the table mentioned in the topic `inet (interfaces)`. When you try to configure same IP on two logical interfaces inside same routing instance, the commit will be blocked with the error displayed as shown below:

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.2/24

[edit]
user@host# commit
commit complete

[edit]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 2.2.2.2/24

[edit]
user@host# commit
[edit interfaces ge-0/0/2 unit 0 family inet]
  'address 2.2.2.2/24'
    identical local address found on rt_inst [default], intfs [ge-0/0/2.0 and ge-0/0/1.0],
    family [inet].
error: configuration check-out failed</screen-output>
```

[See [inet\(interfaces\)](#).]

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](#).]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See [request system scripts refresh-from](#) and [cert-file \(Scripts\)](#).]

Layer 2 Ethernet Services

- **Active leasequery-based bulk leasequery (MX Series)**—The overrides `always-write-option-82` and `relay-option-82 circuit-id` configurations at the `[edit forwarding-options dhcp-relay]` hierarchy level are not mandatory for active leasequery-based bulk leasequery. For earlier releases, the overrides `always-write-option-82` and `circuit-id` configurations are mandatory for active leasequery-based bulk leasequery. For regular bulk leasequery between relay and server without any active leasequery, the overrides `always-write-option-82` configurations are mandatory.

[See [bulk-leasequery \(DHCP Relay Agent\)](#).]

Layer 2 Features

- **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

- **Chef and Puppet support removed (EX Series except EX4400, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, Junos OS products that were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS. FreeBSD 12.x based Junos OS does not support installing existing Chef or Puppet packages.
- **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](#).]

- **Changes to <commit> RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server's response for <commit> operations includes the following changes:
 - If a successful <commit> operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.
 - The NETCONF server response emits the <source-daemon> element as a child of the <error-info> element instead of the <rpc-error> element.
 - If you also configure the `flatten-commit-results` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server suppresses any <commit-results> XML subtree in the response and only emits an <ok/> or <rpc-error> element.

[See [Configuring RFC-Compliant NETCONF Sessions](#).]

- **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 OID ifHighSpeed**—Now, the object identifier (OID) ifHighSpeed displays the negotiated speed once negotiation is completed. If the speed is not negotiated, ifHighSpeed displays the actual maximum speed of the interface. In earlier releases, ifHighSpeed always displayed the actual speed of the interface.

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

Software Defined Networking (SDN)

- **VLAN isolation disabled by default (MX480, MX960, MX2008, MX2010, and MX2020)**—For Junos node slicing, the internal control plane no longer isolates GNFs from each other by default. The internal network has sufficient bandwidth to accommodate GNFs without needing to isolate GNFs from each other. However, if you want to isolate the internal traffic of each GNF from all others, you must configure the `set chassis network-slices vlan-isolation` CLI configuration statement (which is applicable for all uses except with sub line cards) on all the Routing Engines of the BSYS and GNFs and then reboot the chassis. If you want to configure the sub line card feature, you must ensure that VLAN isolation is disabled.

We have deprecated the configuration statement `no-vlan-isolation`.

[See [vlan-isolation.](#)]

VPNs

View the traffic selector type for an IPsec tunnel (SRX Series and MX Series)—You can run the `show security ipsec security-associations detail` command to display the traffic selector type for a VPN. The command displays `proxy-id` or `traffic-selector` as a value for the TS Type output field based on your configuration.

[See [show security ipsec security-associations.](#)]

Known Limitations

IN THIS SECTION

- [EVPN | 143](#)
- [General Routing | 143](#)

- Infrastructure | 144
- MPLS | 145
- Network Management and Monitoring | 145
- Platform and Infrastructure | 145
- Routing Protocols | 145
- User Interface and Configuration | 146

Learn about known limitations in Junos OS Release 21.2R3 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

- EVPN-VXLAN ESI might result minor loop in some scenarios and could hit duplicate address detection (DAD) in IPV6. [PR1619504](#)

General Routing

- RPD slips are noticed on MX104 devices that have large configuration load on the box with multiple services enabled. [For,example I2circuits, VPLS, L3VPN, firewall-filters configuration, and SNMP-polling.] To avoid RPD slips for longer time duration, configure the `delta-export`, `persist-groups-inheritance`, and `fast-synchronize` system configurations. You must reduce configuration size where possible. Remove any trace-options and reduce the logging pressure on the NAND-flash storage. Analyze the load from processes such as `snmpd`, `mib2d`, and `pfed` processes if you run SNMP. [PR1361250](#)
- In case of SyncE signal loss, DPLL3 goes into the `Holdover` state and still the DPLL1/SYNTH1 signal output gets driven to CB. CB DPLL appears to be in the `Locked` state due to which `INVALID QL` gets generated. The output for the `Current clock status` is always taken from CB DPLL state, due to which the status is displayed as `locked`. [PR1509356](#)
- It is possible that LFM might flap during MX-VC ISSU. [PR1516744](#)

- Running the `help apropos` command in the configuration mode causes the `mgd` process to generate a core file. The `mgd` process comes back up and as long as the command does not cause issue, the process does not generate a core file. [PR1552191](#)
- MX Series platforms do not support sFlow egress sampling of MPLS packets. [PR1556659](#)
- The Resource `deadlock avoided` error message gets generated during software add on platforms that support phone-home solution for ZTP. [PR1557468](#)
- On MX Series devices, the TTL value reported by sFlow egress sampling is equal to the TTL prior to decrement. The sFlow sampling at ingress and the sFlow sampling at egress report the same value of TTL. [PR1559565](#)
- The eODN feature supports up to 1000 SRTE LSPs with 32,000 express segment links in TED. [PR1561947](#)
- Dynamic next-hop tunnel statistics occurs on MX Series routers. Statistics for the traffic entering into the tunnel get incremented on the ingress FPC where traffic arrives and telemetry statistics get reported from ingress FPC. [PR1567227](#)
- The PTP FPGA is kept in reset during BIOS boot. During Linux boot, the PTP FPGA is taken out of reset and `pcie-tree` is reenumerated. The Link-up/down occurs during this sequence. [PR1572061](#)
- When you start ISSU, it is expected that the FPC restart does not get triggered by you. The ISSU can be aborted and system can be in-correct state. [PR1572851](#)
- On MX, ISSU or upgrade with `validate` option might fail if there is too less disk space in `/var/tmp/` in Junos. It is recommended to clear out all log files and core files before initiating upgrade with `validate` option (when not using `no-validate` option) or ISSU. It is better to clear all unwanted data using the `request system storage cleanup` command to clean up all unwanted data. You must ensure that there is at least 9 GB free space in `var/tmp` after copying VMHost package file to `/var/tmp/`. [PR1582554](#)
- On deactivating the aggregated Ethernet interface, traffic loss of greater than 2 seconds occurs. This behavior is seen due to order in which the messages are processed in FPC wherein next hop change/delete is processed prior to interface down event. [PR1614508](#)
- The spike in RPD usage is expected because of the very large scale and OCST in general but it should not affect any RPD functionality if that is the concern as telemetry streaming is the least priority task in RPD. [PR1614978](#)

Infrastructure

- When upgrading from Junos OS release 21.2 and earlier to Junos OS release 21.2 and later, validation and upgrade fails. You must upgrade software using the `no-validate` command. [PR1568757](#)

MPLS

- If the Routing Engines are not all rebooted after a network service configuration change, the rpd process might crash. [PR1461468](#)
- With local reversion ON, there is a possibility of transit router not informing headend of RSVP disabled link when link is flapped more than once. As a workaround, remove the local-reversion configuration. [PR1576979](#)
- When there is scaled RSVP sessions [around 21,000] and have enabled RSVP for all the interfaces,RPD process walks through all the interfaces which results into high CPU for some time, which also results LSP flap and log message on the Routing Engine switchovers. [PR1600159](#)
- There is no traffic impact but the show route forwarding-table destination *a.b.c.d* command have stale entry for around 60 seconds. [PR1610620](#)

Network Management and Monitoring

- Junos has a feature to block or deny all hidden commands. Users can get this feature by configuring the set `system no-hidden-commands` statement. However, when this is configured and committed Junos blocks or denies new netconf/junoscript XML sessions. As a workaround, you can delete the `system no-hidden-commands` statement and start the new netconf/junoscript sessions. [PR1590350](#)

Platform and Infrastructure

- In some scenarios with MPC, major alarm and following messages are generated. This major error is triggered due to parity error, and the impacted queue might drop packets. This might impact the forwarding, to recover MPC card need to be rebooted. [PR1303489](#)
- With a sensor being subscribed via Junos Telemetry Interface (JTI), after the interface is deleted/deactivated/disabled, the TCP connection is still established, and the show agent sensors command still shows the subscription. [PR1477790](#)

Routing Protocols

- With max number of IFLs gets generated [4000 GRE tunnel per Packet Forwarding Engine] with following configuration:

- family inet and associated source and destination for each tunnel.
- Configure the allow-fragmentation statement on one endpoint of the tunnel.
- Configure reassemble-packets on the other endpoint of the tunnel.

[PR1581042](#)

User Interface and Configuration

- For the list definition as shown below: `list bar { key foo; leaf foo { type uint8; } leaf baz { type string; } }` Junos cannot parse the below configuration payload where 'leaf foo' (key as per Yang model) does not appear as a first element. `{ "bar": [{ "baz": "zig", "foo": 123 }, { "baz": "zag", "foo": 0 }] }` Junos understands only this kind of configuration payload as shown below where 'leaf foo' (key as per Yang model) appears as a first element. `{ "bar": [{ "foo": 123, "baz": "zig" }, { "foo": 0, "baz": "zag" }] }` As per Junos, the list keys are always required (must always) to precede any other siblings within a list entry and appear in the order specified by the data model. [PR1616216](#)

Open Issues

IN THIS SECTION

- [Class of Service \(CoS\) | 147](#)
- [EVPN | 147](#)
- [Flow-based and Packet-based Processing | 148](#)
- [Forwarding and Sampling | 148](#)
- [General Routing | 148](#)
- [High Availability \(HA\) and Resiliency | 157](#)
- [Interfaces and Chassis | 157](#)
- [J-Web | 157](#)
- [Layer 2 Ethernet Services | 157](#)
- [MPLS | 158](#)
- [Platform and Infrastructure | 159](#)
- [Routing Protocols | 160](#)

- [Unified Threat Management \(UTM\) | 162](#)
- [User Interface and Configuration | 162](#)
- [VPNs | 163](#)

Learn about open issues Junos OS Release 21.2R3 for MX Series routers.

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

Class of Service (CoS)

- On MX platforms, deactivating or activating the target-mode using the `set chassis satellite-management fpc target-mode` command leads to a bad state at the Packet Forwarding Engine on the extended ports, which leads to traffic disruption. [PR1593059](#)
- On MX platforms with MPC10 and MPC11 line cards, if you apply Class-of-Service (CoS) `ieee-802.1` rewrite rule on the aggregated Ethernet interface with VLAN circuit cross-connect encapsulation, the rewrite rule might not work as expected. [PR1604943](#)

EVPN

- A few duplicate packets might be seen in an A/A EVPN scenario when the remote PE device sends a packet with an IM label due to MAC not learned on the remote PE device, but learned on the A/A local PE device. The nondesignated forwarder sends the IM-labeled encapsulated packet to the PE-CE interface after MAC lookup instead of dropping the packet, which causes duplicate packets to be seen on the CE side. [PR1245316](#)
- With Junos OS Release 19.3R1, VXLAN OAM host-bound packets are not throttled with DDoS policers. [PR1435228](#)
- In PBB-EVPN (Provider Backbone Bridging - Ethernet VPN) environment, ARP suppression feature which is not supported by PBB might be enabled unexpectedly. This might cause the MAC addresses of remote CEs not to be learned and hence traffic loss. [PR1529940](#)

- EVPN-MPLS multi-homing control MACs are missing after vlan-id removal and adding back on a trunk IFL of one of the multi-homing PEs. This is not a recommended way to modify vlan-id configuration. Always both MH PE devices must be in symmetric. [PR1596698](#)
- Issue occurs with translation VNI when MAC moved one from DC1 to DC2. VM move across DC where there is not translate VNI configuration in the interconnect works as expected. [PR1610432](#)
- EVPN Local ESI MAC limit configuration might become effective immediately when it has already learned remote MH Macs. Clear the Mac table from all MH PE devices and configure the MAC limit over the local ESI interfaces. [PR1619299](#)

Flow-based and Packet-based Processing

- You can 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](#)

Forwarding and Sampling

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

General Routing

- AFEB crashes with PTP thread hog on the device. Through it fixes the PTP packet processing when PTP is enable, which is when PTP configuration is active. If the PTP configuration is not there, PTP packet processing is ignored even if FPGA displays PTP packet is available. [PR1068306](#)
- On MX104 devices, when RE CPU usage is going high, sporadic I2C error message gets generated. The I2C access might succeed in the next polling. [PR1223979](#)
- If a vmhost snapshot is taken on an alternate disk and there is no further vmhost software image upgrade, the expectation is that if the current vmhost image gets corrupted, the system boots with the alternate disk so the user can recover the primary disk to restore the state. However, the host root file system and the node boots with the previous vmhost software instead of the alternate disk. [PR1281554](#)

- Backup Routing Engine might crash after GRES occurs continuously for more than 10 times. [PR1348806](#)
- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter does not get installed. [PR1362609](#)
- Due to transient hardware condition, single-bit error (SBE) events are corrected and have no operational impact. Reporting of those events had been disabled to prevent alarms and possibly unnecessary hardware replacements. This change applies to all Platforms using Hybrid Memory Controller (HMC). [PR1384435](#)
- Due to a timing issue during the sxe interface bring up (w.r.t i40e driver). Recovery can be done by rebooting the complete board. [PR1442249](#)
- In race condition, 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 might crash. [PR1458595](#)
- Either static routes (or) implicit filters should be configured for forwarding DNS traffic to service pic. It solves DNS packet looping issue. [PR1468398](#)
- Currently, IP options are not supported for egress firewall attach points. The issue might occur in the IP-options router alert traffic not hitting the egress firewall filter. [PR1490967](#)
- On MX204 and MX10003 routers, MPCs MPC7E through MPC10E, and JNP10K-LC2101, an error syslog unable to set line-side lane config (err 30) might be generated. [PR1492162](#)
- 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](#)
- After backup Routing Engine halt, CB1 goes offline and comes back online causing the backup Routing Engine to boot up and generate the `0x1:power cycle/failure` message. [PR1497592](#)
- On all platform with BGP SR-TE (Spring-TE), in the SR topology the transit IPv4 traffic might have missing labels and might get dropped in first hop, when ingress is forwarding traffic. All labels might be missed out except the last hop in the v4 traffic forwarded by nexthop interface. [PR1505592](#)
- On a fully scaled system where all the slices are utilized by different families of CLI filters, if you try to call delete for one family and add/change for another family with a higher number of filter terms, which requires either expansion of the filter or creation of a new filter, the Packet Forwarding Engine fails to add the new filter. [PR1512242](#)
- A delay of 35 seconds gets added in reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. [PR1514364](#)
- Active sensor check fails while issuing the `show agent sensors | display xml` command. [PR1516290](#)

- When you configure an AMS ifd for the first time or any member of the AMS bundle is removed or added, the PICs on which the members of AMS bundle are present go for a reboot. There is a timer running in the AMS kernel which is used as a delay for the PIC reboot to complete and once that timer expires AMS assumes that the PICs might have been rebooted and it moves into next step of AMS fsm. In scaled scenarios, this rebooting of the PIC is delayed due to DCD. This is because when a PIC goes down, DCD is supposed to delete the IFDs on that PIC and then the PIC reboot happens. But DCD is busy processing the scaled config and the IFD deletion is delayed. This delay is much greater than the timer running in AMS kernel. When the above timer expires, the FSM in AMS kernel wrongly assumes the PIC reboot would be completed by then, but the reboot is still pending. By the time DCD deletes this IFD the AMS bundles are already UP. Because of this, there is a momentary flap of the bundles. [PR1521929](#)
- On the MX platforms with NG-RE installed, after upgrading the Intel i40e-NVM firmware to version 6.01, the FRUs disconnection alarms may be seen along with traffic loss. [PR1529710](#)
- Due to BRCM KBP issue route lookup might fail. [PR1533513](#)
- After performing ISSU (In-Service Software Upgrade) on the Junos node slicing, the ISSU unsupported FRU (Field Replaceable Unit) stays offline until bringing online manually once ISSU finishes. This issue causes a service/traffic impact for the offline FRUs. [PR1534225](#)
- The request system software validate command gets disabled currently from Junos OS Release 19.4 and later. Use the request system software add command to validate. [PR1537729](#)
- If the Packet Forwarding Engine processes distributed IGMP pseudo ifl delete, it attempts to delete all associated multicast flows. On a scaled setup, deleting several thousand multicast flows hogs CPU for long time that gets killed by the scheduler, resulting in generating core file. [PR1537846](#)
- The Socket to sflowd closed error message 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 scaled MX2020 router, with vrf localisation enabled, 4 million nexthop scale, 800,000 route scale. FPCs may go offline on GRES. Post GRES, router continues to report many fabric related CM_ALARMS. FPC may continue to reboot and not come online. Rebooting the primary and backup Routing Engine helps to recover and get router back into stable state. [PR1539305](#)
- Broadcom has updated that BCMX calls are deprecated and needs to be replaced with BCM calls. [PR1541159](#)
- 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](#)
- Hardware performance counters may not be correctly exported to the CLI when the Packet Forwarding Engine gets disabled. [PR1547890](#)

- Validation of OCSP certificate may not go through for some CA servers using openssl . In some cases, when we get the ca address using getaddrinfo(), the gataddrinfo() api returns multiple entries of the same ca address. Due to this pkid creates multiple socket connections to the same CA and goes into busy state. [PR1548268](#)
- 100G AOC from Innolight does not comes up after multiple reboots.It recovers after interface enables or disables. [PR1548525](#)
- The issue applies to the initial release of CBNG for 22.1. Running the help apropos command in the configuration mode causes an MGD core. The MGD comes back up and as long as the command is not issues again the core will not occur. [PR1552191](#)
- When the telemetry data for a node which is streamed is deleted during a network churn and the same node is being walked/rendered for the sensor, RPD might core dump. This is a corner case where the rendering and deletion of a particular node has to happen at the same instance. This issue can occur only in case of a unstable network. [PR1552816](#)
- 5M DAC connected between QFX10002-60C and MX2010 doesn't link up. But with 1M and 3M DAC this interop 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/bridge-domain add, flood tokens and routes are created for both VE and CE mesh-group/flood-group. Ideally, VE mesh-group doesn't require on a CE router where IGMP is enabled on CE interfaces. [PR1560588](#)
- Due to a race condition, the output of the show multicast route extensive instance instance-name command displays the session status as invalid. [PR1562387](#)
- To avoid the additional interface flap, interface hold time needs to be configured. [PR1562857](#)
- In a rare scenario, SPMB does not reply during FPC online which was moved from SLC mode to full line card mode. [PR1563050](#)
- When SLC is reconfigured from asymmetric mode to symmetric mode in a single commit it is possible that on some occasions one of the SLC shows chassis connection dropped state. The SLC becomes online. [PR1564233](#)
- Starting Junos OS Release 21.1R1, Junos OS ships 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, so far (until 20.4R1), the python script had #!/usr/bin/python as the first line (the path of the python interpreter). The same needs to be changed to #!/usr/bin/python3 from 21.1R1 [PR1565069](#)

- In Dual CPE scenario, after RGO failover, the best path link status displayed as PARTIAL SLA VIOLATED instead of SLA MET due to active probe result gone wrong in certain scenarios. [PR1565777](#)
- During the ingress processing we maintain separate counters for Layer 2 unicast, multicast, and broadcast as well as for unknown unicast. Whereas during egress processing we only maintain the ifl level stats after the wan out. Hence, at egress level output multicast counter always shows 0. [PR1566436](#)
- 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](#)
- In an external server-based Junos Node Slicing scenario, the logical partitions (called sub line cards or SLCs) can be additionally configured for MX2K-MPC11E and assigned to different guest network functions (GNFs). If the inline services and services are applied to SLCs, some issues might happen during processing these services along with firewall process (dfwd) filter actions. It might cause SLCs to reboot and aftd crash. [PR1567313](#)
- Packet Forwarding Engine error message Tunnel id: does not exist gets generated while executing the show dynamic-tunnel database statistics command 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](#)
- In MX Series devices, the device may not send pause frames in case of congestion. [PR1570217](#)
- Copying files to /tmp/ causes a huge JTASK_SCHED_SLIP. 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 because the primary Routing Engine and secondary Routing Engine are out of syncing dcd.snmp_ix information. [PR1571677](#)
- On all Junos platforms, traffic loss might be observed due to a rare timing issue when performing frequent IFBD (Interface Bridge Domain) 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](#)
- After Junos OS upgrade, MAC address changes will be seen on MPC9E PIC1 interfaces. Static MAC configurations will be affected. [PR1575009](#)
- Max ports used is not getting displayed properly in the show services nat pool pool-name detail command. [PR1576398](#)
- On MX platforms, in subscriber scenario with scaled around 32,000 connections, the Replication Daemon might generate core files or stop running, which results in failure on subscriber services on

the new RE after the upgrade/GRES. The fix is to increase the max capacity of the ifl Stats DB shared memory. [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 config is committed the block creation utilizes more memory causing NAT pool memory shortage which is currently being notified to customer with syslog tagged RT_NAT_POOL_MEMORY_SHORTAGE. [PR1579627](#)
- In a fully loaded devices, at times, firewall programming was failing due to scaled prefix configuration with more than 64,800 entries. However, this issue is not observed in development setup. [PR1581767](#)
- If a BSYS Routing Engine switchover is triggered by simulating a kernel crash on a node-sliced platform, the FPCs or SLCs stay in present state while the related GNFs become unreachable. A system reboot is required to resolve this issue. This issue is seen only in the MX2020 platform with the REMX2K-X8-128G Routing Engine. [PR1584478](#)
- COS classifiers and rewrites not supported on a logical tunnel (LT interface) with Ethernet-CCC or Ethernet-bridge encapsulation. COSD does not prevent a commit but then the classifiers/rewrites are not bound to the LT interface at PFE and hence wont work. Sample configuration: set interfaces lt-11/0/0 unit 0 encapsulation ethernet-ccc set interfaces lt-11/0/0 unit 0 peer-unit 1 set interfaces lt-11/0/0 unit 0 statistics set interfaces lt-11/0/0 unit 1 encapsulation ethernet-bridge set interfaces lt-11/0/0 unit 1 peer-unit 0 set interfaces lt-11/0/0 unit 1 statistics set bridge-domains data vlan-id none set bridge-domains data interface lt-11/0/0.1 set bridge-domains data interface xe-11/0/3:2 set protocols l2circuit neighbor 1.1.2.1 interface lt-11/0/0.0 virtual-circuit-id 100 set class-of-service interfaces lt-11/0/0 forwarding-class expedited-forwarding Attaching fixed classifier to LT tunnel interface where the tunnel carries etherent-ccc/ethernet-bridge encapsulation. [PR1585374](#)
- With preserve hierarchy statement ON and option c is used with BGP CT, the VPN CT stitching routes at ASBR if resolving over an SRTE tunnel having single label. Then, the forwarding mpls.0 route programming will be incorrect on MX boxes. [PR1586636](#)
- The rpd process generates core file at rt_iflnh_set_nhid. Core is due to assertion caused by failure of hbt_insert for nhid belonging to an ifl. It is seen that there is a duplicate entry present which causes the hbt_insert failure. [PR1588128](#)
- Transient Traffic drop will be seen during MBB of RSVP LSP without "optimize-adaptive-teardown delay 60" knob [PR1590656](#)
- On all devices running Junos OS Release 19.1R3-S5-J3, the subscriber IFL(logical interface) might be in a stuck state after the ESSM (Extensible Subscriber Services Manager) deletion. [PR1591603](#)
- On DUT with MPC11E linecard and scaled pseudowire headend termination configs,on performing iterative enhanced mode ISSU, PPE(packet processing engine) traps and BGP peer flaps are seen.

These result in transient traffic loss of several minutes on DUT. traps and protocols flaps are NOT seen in first iteration, but subsequent iterations. RE and linecards are NOT rebooted between enhanced mode ISSU iterations. [PR1593335](#)

- On a node sliced platform with mpc11e sliced into Sub Line cards it is possible that the syslog messages displays the error message `aftd-trio[13014]: [Error] IF:IfdCfgMsg, ifd not found, ifdIndex:2399`, when GNF has configuration that does not pertain to the Packet Forwarding Engines. [PR1594816](#)
- On all MX platforms, changing configuration AMS 1:1 warm-standby to load-balance or deterministic NAT may result in vmcore and cause traffic loss. [PR1597386](#)
- Continuous offline/online of FPC multiple times can result into FPC restart at init state causing additional 2min in boot time. [PR1599469](#)
- The `show chassis fabric plane` command might display incorrect plane status in some cases when injecting fec errors. [PR1600187](#)
- In some instances, when FHP recovery action is performed on an SLC due to blackholing, the restart operation on the SLC may result may not be successful and the FHP recovery action may timeout. [PR1600559](#)
- Frame stack messages are seeing during MPC11E subLC boot up, when subLC is added to GNF. [PR1600749](#)
- 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 hold-time for up and down helps to resolve. [PR1601946](#)
- In Junos OS Release 21.1R2 and Junos OS Release 21.1R3, in chassis with mix of MPC10 or MPC11 and MPC1 to MPC9, and AE bundle configuration with member links on both MPC10/MPC11 and MPC1-MPC9, packet loss may be seen for unicast packets on link flap using `ifconfig down/up` command in the Routing Engine shell. [PR1604073](#)
- During the Routing Engine switchover if there is a burst of ICMP/BFD/SSH/FTP/TELNET/RSVP packets (around 18,000 pps), new backup Routing Engine restarts. [PR1604299](#)
- On aggregate Ethernet interfaces with some of the member links part of MPC10 or MPC11, and other member links part of other MPC type (MPC1 up to MPC9), if you delete an "ae" interface, other "ae" interfaces may experience unicast packet loss. [PR1604450](#)
- In Junos OS Release 21.1R2 and Junos OS Release 21.1R3, in chassis with mix of MPC10 or MPC11 and MPC1 to MPC9, and AE bundle configuration with member links on both MPC10/MPC11 and MPC1-MPC9, packet loss might be seen for unicast packets on link flap using `deactivate bundle/activate bundle`. [PR1604800](#)
- In Junos OS Release 21.1R2 and 21.1R3 release, in chassis with mix of MPC10 or MPC11 and MPC1 to MPC9, and AE bundle configuration with member links on both MPC10/MPC11 and MPC1-

MPC9, packet loss may be seen for unicast packets on link flap using ifconfig down/up command in the Routing Engine shell. [PR1604814](#)

- When fabric plane offline/online may results in destination error on line cards. [PR1605770](#)
- On the MX240, MX480, and MX960 system with both MPC10E and MPC2, MPC3, MPC4, MPC5, and MPC6 based FPCs are installed, when MPC10E sends high traffic to MPC4E or other mentioned cards as the destination, the destination line card will not be able to cope up with MPC10E traffic flow. [PR1606296](#)
- Issue occurs when there is an Packet Forwarding Engine error causing disable-pfe, not seen in the normal FRR switchover. [PR1609768](#)
- Output of the show network agent command should be null, which shows statistic per component after GRES. [PR1610325](#)
- In MX240, MX480, and MX960 platforms with SCBE3-MX and Enhanced midplane scenario, in some rare cases, if flooding huge traffic from MPC7, MPC8, and MPC9 to MPC2E, MPC3E, MPC4E, MPC5E and flapping the interface on MPC2E, MPC3E, MPC4E, and MPC5E, it will cause the unexpected request time errors on MPC7, MPC8, MPC9 since the MPC2E, MPC3E, MPC4E, MPC5E might not be able to handle such high volume of requests, it will cause PFE destinations to become unreachable even when the fabrics are online. Then PFE/SIB/SCBE/FPCs might reboot automatically while these accumulated fabric errors hit the fabric connectivity restoration conditions of the Fabric Healing process (FHP). [PR1612957](#)
- In some NAPT44 and NAT64 scenarios, duplicate SESSION_CLOSE syslog message gets generated. [PR1614358](#)
- On MX-SPC3 platform, a memory corruption is occurring in the iked daemon occasionally when ams interfaces are used in service-set configuration. Issue is occasionally seen in 21.2R2.4. Issue not seen at all from 21.2R2.8 onwards. [PR1620115](#)
- When installing an IPv6 firewall filter using BGP flowspec, matching traffic counters displays 0 values. [PR1623170](#)
- When traffic selector (optional parameter) and bind interface (required parameter) is configured for a vpn profile and static route is configured for the same remote ip (mentioned in the traffic selector) with same next-hop interface (mentioned in the bind-interface) on MX-SPC3 devices, then the static route takes preference over the route installed by the ipsec daemon (iked) based on the traffic selector, which causes data traffic loss as the packets are routed via the wrong route. [PR1624062](#)
- On Junos OS Release 21.1R2.4, an issue has been introduced on the flowd (service-card) side where any protocol packet expect for TCP/UDP/ICMP/ICMPV6 gets dropped when NAT translation doesn't happen. The mentioned bug has been fixed from 21.2R2.8 junos version onwards. [PR1624063](#)

- On MX platforms that use MPC11E cards, when fast-lookup-filter is enabled, traffic drop might be seen in the node slicing scenario. [PR1626115](#)
- On MX Series platforms with MPC10/MPC11 and MS-MPC/MS-MIC are used, if aggregated multiservices (AMS) interface is configured as next-hop with equal-cost multipath (ECMP), load balancing will not happen properly according to source-ip hashing. [PR1628076](#)
- Bad IP length packets (ip header length field > actual packet size) when encapsulated within MPLS are dropped as expected, but might trigger PPE traps in some cases. [PR1628091](#)
- Zeroize RPC returns no positive reply. [PR1630167](#)
- On MX platform 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. Service impact is minor or negligible as the TFTP control session will eventually get deleted after timeout. [PR1633709](#)
- On all MX platforms, when the interface (xe-0/0/x) is equipped with a QSA module, only channel 0 (xe-0/0/x:0) is supported and channels 1 to 3 are not supported, though they show up in the show interface command. But disabling laser for one of these non-supported channels puts the entire optics in low power. As a result, transmit power of channel 0 becomes 0 and the link goes down. [PR1636874](#)
- On Junos platforms equipped with MPC10E/MPC11E/LC2301/MX10K-LC9600 line cards, when any 100G/400G interface with high priority class-of-service scheduler configuration flaps, it might result in series of error messages during high traffic flow. Eventually this would result in PFE-disable action, impacting the related traffic. However, the issue could be recovered after FPC reboot. [PR1638410](#)
- USB installation requires a keypress before reboot to enable removal of USB device before system is restarted. Failing to remove USB stick will cause installation to start again. This fix prompts user for a keypress after installation and before reboot. [PR1640143](#)
- JDHPCD core dump occurs when client attempts connection on pseudowire for dhcp-relay after JUNOS upgrade. [PR1649638](#)
- On MX480 routers, remote-mep-state does not work as expected. [PR1623960](#)
- When ip-fix transfers telemetry files and ntf-agent daemon closes or restarts, there could be a core with the backtrace (CRYPTO_THREAD_unlock). The daemon recovers by itself. [PR1617568](#)
- In the MVPN case, if the nexthop index of a group is not the same between the primary and backup after a nsr switchover, we might see a packet loss of 250 to 400 ms. [PR1561287](#)
- On MX480 router, during the verification of GRES and NSR functionality with VXLAN feature, the convergence is not as expected Layer 2-DOMAIN-TO-Layer 3 VXLAN. [PR1561287](#)

High Availability (HA) and Resiliency

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

Interfaces and Chassis

- On all Junos platforms with broadband subscriber management protocols being implemented, when redundant logical tunnel interface[rlt0] having 2 member interfaces in 2 different FPCs and it is used as the anchor point for the pseudo subscriber interface[ps0] in an event which can bring the primary member interface down, traffic is not failed over to the backup interface. [PR1492864](#)
- When family bridge is configured, IFLs are not created. If IFLs are not created, l2ald does not create IFBDs (interface to BD association) and if we don't have IFBDs in the system, STP is not enabled on that interface. [PR1622024](#)

J-Web

- The Firefox browser displays an unsaved changes error message in the J-Web Basic Settings page if the Autofill logins and passwords option is selected under the Browser Privacy and security settings. [PR1560549](#)

Layer 2 Ethernet Services

- On MX5/MX10/MX40/MX80/MX104 Series platforms with DHCP server configuration for DHCP subscribers, the jdhcpd memory leak might happen and the memory increase by 15MB which depends on the number of subscribers when testing the DHCP subscribers log-in/out. [PR1432162](#)
- If the request system zeroize command does not trigger zero-touch provisioning, please re-initiate the ZTP as a workaround [PR1529246](#)
- On MX Series platforms, there may be a mismatch in subscriber information between the devices when the two devices are configured as Dynamic Host Configuration Protocol (DHCP) relay Active lease Query (ALQ) peers. This is a timing issue that occurs frequently when the lease timer is less than 300secs. [PR1638050](#)

MPLS

- Bfd session flaps during ISSU only in MPC7E card(Bfd sessions from other cards of DUT to peer routers did not flap during ISSU). Issue is not seen frequently. [PR1453705](#)
- Single hop BFD sessions can sometimes flap after GRES in highly scaled setups which have RSVP link or link-node-protection bypass enabled. This happens because sometimes RSVP neighbor goes down after GRES if RSVP hellos are not received after GRES before neighbor timeout happens. As a result of RSVP neighbor going down, RSVP installs a /32 route pointing to bypass tunnel which is required to signal backup LSPs. This route is removed when all lspd stop using bypass after link comes back up. The presence of this /32 route causes BFD to flap. [PR1541814](#)
- As the update-threshold configuration changes from an attribute to an object between Junos OS Release 18.2X75-D65 and Junos OS Release 18.2X75-D521, the user will need to delete the update-threshold stanza and re-configure it after the downgrade. [PR1546447](#)
- The rsvp interface update threshold configuration syntax has changed between Junos OS Release 18.2X75-D435 and Junos OS Release 20.3X75-D10 to include curly braces around the threshold value. Upgrading and downgrading between these releases is not entirely automatic. The user must delete this stanza if configured before the downgrade and then manually reconfigure. [PR1554744](#)
- In MVPN Case, if the nexthop index of a group is not same between master and backup after a nsr switchover, we may see a packet loss of 250 to 400 ms. [PR1561287](#)
- If IS-IS-TE or OSPF-TE is enabled, but extended admin groups (which is configured under routing-options) are configured after the peer router advertises the extended admin groups, the LSP with extended admin groups constraints might fail to be established. [PR1575060](#)
- The use-for-shortcut knob is meant to be used only in SRTE tunnels which use SSPF (Strict SPF Algo 1) 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 SRTE tunnel using Algo 0 Prefix SIDs is configured with "use-for-shortcut" knob, it could lead to routing loops or rpd cores. [PR1578994](#)
- When there is scaled RSVP sessions [~21K] and have enabled RSVP for all the interfaces,RPD process walks through all the interfaces which results into high CPU for some time, which also results LSP flap. [PR1595853](#)
- When there is scaled RSVP sessions [~21K] and have enabled RSVP for all the interfaces,RPD process walks through all the interfaces which results into high CPU for some time, which also results LSP flap, will see the log message on RE switch over,due to this protocols also can flap. [PR1600159](#)
- There is no traffic impact but the show route forwarding-table destination < a.b.c.d> command, contains stale entry for around 60 seconds. [PR1610620](#)

- If LSP reoptimization is enabled for the primary and secondary path that is standby, the standby secondary LSP might get stuck on the same path as primary LSP after network change that triggers reoptimization happens. [PR1615326](#)
- 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](#)

Platform and Infrastructure

- MPLS traffic going through the ingress pre-classifier logic may not determine MPLS payload correctly, classifying MPLS packet into control queue versus non-control queue and exposing possible packet re-order. [PR1010604](#)
- The commit synchronize command fails because the kernel socket gets stuck. [PR1027898](#)
- On MX-Series platforms with MPC7/8/9 or MX-204/MX-10003 when the packets which exceed the MTU and whose DF-bit is set go into a tunnel (such as GRE, LT), they might be dropped in the tunnel egress queue. [PR1386350](#)
- The traps are the result of PPE commands injected from the host. One possible reason could be Layer 2 BD code, which is trying to decrement BD MAC count in the data plane. It is unlikely that there is a packet loss during this condition. This could happen during ISSU and this may be due to a problem with ISSU counter morphing used for LU-based cards, where certain counters are not disabled or disabled too late during ISSU. [PR1426438](#)
- Arrival rates are not seen at system level when global-disable fpc is configured on qfx [PR1438367](#)
- Due to software implementation, firewall filter is re-applied during graceful switchover (GRES). This may lead to short duration when filter is not applied to the provoking side effects like drop of traffic. [PR1487937](#)
- With GRES and NSR functionality with VXLAN feature, the convergence time may be slightly higher than expected for L2-DOMAIN-TO-L3VXLAN [PR1520626](#)
- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect asic programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. [PR1530160](#)
- This issue notes an impact to RPM behavior in non-delegate mode with MPC10 line cards. It is observed that the RPM packets from client are received and processed by RPM server but the response packets are dropped before they are received by the client. [PR1556697](#)

- On MX Series devices and the EX9200 line of switches, the FPC gets restarted and thereby disrupts traffic when there is an out-of-order filter state and terms. This issue might be seen only in back-to-back GRES in more than 40 to 50 iterations. [PR1579182](#)
- The issue is due to output byte count not getting updated properly. The script logs shows that there is no packet loss, There is no functional impact and will be taken up in the upcoming releases. [PR1579797](#)
- On MX platforms, during reboot, the AE ifls are first added, then deleted and again added, this flapping causes corner case where the filter attachment ipc has older AE ifl index on which the filter bind fails. Filter will not be attached to the interface, so any filter related service will not work. [PR1614480](#)

Routing Protocols

- While interoperating with other vendors in a draft-rosen multicast VPN, by default 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 is prevented from propagating if the BGP route-target filtering is enabled on the device running Junos OS. [PR993870](#)
- Certain BGP traceoption flags (for example, "open", "update", and "keepalive") might result in (trace) logging of debugging messages that do not fall within the specified traceoption category, which results in some unwanted BGP debug messages being logged to the BGP traceoption file. [PR1252294](#)
- LDP OSPF are in synchronization state because the IGP interface is down with ldp-synchronization enabled for OSPF. user@host> show ospf interface ae100.0 extensive Interface State Area DR ID BDR ID Nbrs ae100.0 PtToPt 0.0.0.0 0.0.0.0 0.0.0.0 1 Type: P2P, Address: 10.0.60.93, Mask: 255.255.255.252, MTU: 9100, Cost: 1050 Adj count: 1 Hello: 10, Dead: 40, ReXmit: 2, Not Stub Auth type: MD5, Active key ID: 1, Start time: 1970 Jan 1 00:00:00 UTC Protection type: None Topology default (ID 0) -> Cost: 1050 LDP sync state: in sync, for: 00:04:03, reason: IGP interface down config holdtime: infinity. As per the current analysis, the IGP interface goes down because although LDP notified OSPF that LDP synchronization was achieved, OSPF is not able to take note of the LDP synchronization notification, because the OSPF neighbor is not up yet. [PR1256434](#)
- In rare cases, RIP replication might fail as a result of performing NSR Routing Engine switchovers when the system is not NSR ready. [PR1310149](#)
- On MX platforms, unexpected log message will appear if the CLI command 'show version detail' or 'request support information' is executed: test@test> show version detail *** messages *** Oct 12

12:11:48.406 re0 mcsnoopd: INFO: krt mode is 1 Oct 12 12:11:48.406 re0 mcsnoopd: JUNOS SYNC private vectors set [PR1315429](#)

- SCP command with Routing Instance (-JU) is not supported. [PR1364825](#)
- On all platforms with a large-scale BGP setup (e.g. advertising 300K routes over 500 BGP peers), high CPU utilization (close to 100%) by BGP I/O thread on master RE might be seen for a couple of minutes (like 10 minutes), which may lead to dramatic performance degradation and even traffic loss if NSR is enabled while there is a lot of advertisements and the backup RE is busy (performing "clear bgp neighbor all" on the RR can achieve this). [PR1488984](#)
- 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](#)
- In previous versions of RFC 9072's draft-ietf-idr-bgp-ext-opt-param, the optional-parameter length was required to be 255 in order to trigger the updated behavior. Later editions of the Internet-Draft permitted non-zero optional parameter length values to be used to support this feature. [PR1554639](#)
- post configuration change commit, due to race on ordering of routing-instance parsing, and rt-export module processing, rt-export may act on stale handle pointing to the previous incarnation of transport-class auto-created instance. Hence it causes the issue in this PR. [PR1556632](#)
- A single hop BFD session over IRB interface works in centralised mode if the VPLS instance the IRB belongs to has only LSI interfaces bound to VPLS pseudowires and has no local non-tunnel attachment circuits. PPMd daemon responsible for the session distribution to FPC microkernel will be attempting to distribute the session indefinitely failing every time. Upon every distribution failure, the following counter increases by 1, typical counter increase rate is about +40 per minute: > user@router> show ppm distribution-statistics > > PPMd distribution statistics: > PFE not eligible: 0 > Kernel returned no address: 340 Client hash index fail: 0 > PFE marked for deletion: 0 > Client eligibility fail: 0 > PFE is not capable: 0 > DFWD is not capable: 0 > Lo0 subunit missing: 0 This issue could be seen on any JUNOS release/platform supporting distributed or inlined single hop BFD over IRB. Both session distribution failure and endless failing attempts to distribute it are expected to be addressed in JUNOS, there is no confirmed date of the fixes arrival. General centralised mode recommendations like avoiding aggressive subsecond BFD timers are applicable to this case. [PR1563947](#)
- Multicast traffic is hogging the switch core when igmp-snooping is removed. The MCSNOOPD will be cored due to the changes in mrouter interfaces and routes [PR1569436](#)
- If the Junos config contains a SHA-1 hashed password for a specific user, that user will be unable to login post upgrade. To identify any SHA-1 hashed passwords, run the following from the edit command line: # show | match \ \$sha1\\$ Post upgrade do not use the SHA-1 password format. If the password format is set to SHA-1, the password will be hashed with SHA-512 instead. [PR1571179](#)
- If OSPF and RSVP are configured, a device that is out of service is transmitting a large number of link-state advertisement (LSAs) (more than 100k), extremely busy neighbors are slow in sending

LSACKs, and some LSA churn happens caused by route flaps, then unexpected CSPF link down/ deleted events happen on LSPs. This causes other OSPF routers in the OSPF domain to fail their CSPF calculation for the router loopbacks that act as P routers in this topology and thus drop the LSPs, causing traffic impairment. In addition, rpd utilization will be pegged to 100%. [PR1576818](#)

- Traffic loss is seen across the LDP path during traffic shift from one router to another device in the MPLS cloud. Two routers with two different capacities converge at two different times, so a microloop occurs between the two nodes. See workaround provided. [PR1577458](#)
- With max number of IFLs [4K GRE tunnel per PFE] with following configuration. 1.> family inet and associated source and destination for each tunnel 2.> Configure allow-fragmentation knob on one endpoint of the tunnel and configure reassemble-packets on the other endpoint of the tunnel As above configuration, if we do "deactivate chassis fpc slot", we may hit this issue. We are still doing analysis to find out root cause of this issue. [PR1581042](#)
- When mpls traffic-engineering and rib inet.3 protect core knob is enabled then transport routes in inet.3 will not be used for route resolution [PR1605247](#)
- When ip-fix is transferring telemetry files and ntf-agent daemon is closed/restarted there could be a core with the backtrace (CRYPTO_THREAD_unlock). The daemon recovers by itself. [PR1617568](#)
- On all Junos OS platforms, traffic might continue to forward on the aggregated Ethernet interface member link even if MicroBFD(Bidirectional Forwarding Detection) status is in a hold-down state. [PR1624085](#)

Unified Threat Management (UTM)

- UTM web-filtering statistics: Total requests: 0 White list hit: 1 Black list hit: 1 Default action hit: 1 Added this field to show display counter for default action hit Custom category permit: 1 Custom category block: 1 Custom category quarantine: 0 Custom category quarantine block: 0 Custom category quarantine permit: 0 Safe-search redirect: 0 Safe-search rewrite: 0 Web-filtering sessions in total: 128000 Web-filtering sessions in use: 0 Fallback: log-and-permit block Default 0 0 Timeout 0 0 Connectivity 0 0 Too-many-requests 0 0 [PR1570500](#)

User Interface and Configuration

- The commitd process might generate core file when issuing the load override statement after DB resize. [PR1569607](#)

- On all Junos OS platforms, when copy-config, get-configuration, discard-change RPCs run in two parallel NETCONF sessions and the database is also accessed in parallel by two NETCONF sessions, it leads to database corruption and mgd related services might crash. [PR1641025](#)

VPNs

- In some scenario (e.g configuring firewall filter) sometimes srx5K might show obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. [PR1432925](#)
- BGP and PIM should have default preference since backup MVPN will choose PIM route based on higher preference only. If BGP is preferred over PIM then PIM route will not be accepted on backup RE. [PR1578164](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.2R3 | 163](#)
- [Resolved Issues: 21.2R2 | 179](#)
- [Resolved Issues: 21.2R1 | 194](#)

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R3

IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 164](#)
- [Class of Service \(CoS\) | 164](#)
- [EVPN | 165](#)

- Flow-based and Packet-based Processing | 165
- Forwarding and Sampling | 165
- General Routing | 166
- High Availability (HA) and Resiliency | 173
- Interfaces and Chassis | 173
- Juniper Extension Toolkit (JET) | 174
- Junos Fusion Provider Edge | 174
- Layer 2 Ethernet Services | 174
- MPLS | 175
- Multicast | 175
- Network Management and Monitoring | 175
- Platform and Infrastructure | 176
- Routing Policy and Firewall Filters | 176
- Routing Protocols | 177
- Services Applications | 178
- Subscriber Access Management | 178
- User Interface and Configuration | 179
- VPNs | 179

Application Layer Gateways (ALGs)

- The flowd daemon will crash if the SIP ALG is enabled and specific SIP messages are processed. [PR1604123](#)
- The flowd process generates core file if the SIP ALG is enabled and a specific Session Initiation Protocol (SIP) packet is received. [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 could lead to traffic control profile on the interface-set error. [PR1593058](#)

- The fabric queues priority might not get changed after activate/deactivate CoS configuration. [PR1613541](#)

EVPN

- Baseline EVPN-VXLAN Transition from IPV4 to IPV6 or vice verse 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](#)
- Transit Traffic gets dropped post disabling one of the PE-CE link on a remote Multi-Home PE in EVPN-MPLS A-A setup with Dynamic-List NextHop configured. [PR1594326](#)
- Bridge mac-table learning entries might not be as expected for the EVPN-MPLS routing instance. [PR1600310](#)
- Few ARP/ND/MAC entries for Vlans are missing with MAC-VRF configuration. [PR1609322](#)
- Missing MAC address entries in EVPN mac-table despite the presence of the corresponding Type 2 route. [PR1611618](#)
- The l2ald crash might be seen after performing restart routing on EVPN PE. [PR1629426](#)
- Removing the es-label-oldstyle statement does not take effect if it is the only knob configured under the protocol EVPN. [PR1629953](#)
- The rpd might crash when moving an interface from VPLS to EVPN-VPWS instance. [PR1632364](#)
- The traffic loss might be seen when the link goes down for the local ESI. [PR1632723](#)

Flow-based and Packet-based Processing

- Unable to execute `/usr/sbin/picinfo: dad file descriptor while issuing the clear services inline-monitoring statistics command.` [PR1624094](#)

Forwarding and Sampling

- The IPv6 filter for family bridge cannot be referenced onto IFL. [PR1598530](#)
- Delay in getting the response for the `clear interfaces statistics all` command with scale configuration. [PR1605544](#)
- Commit is allowed even if firewall filter is not applied to the FPC. [PR1618231](#)
- The FPC might crash when interface participating in the next-interface filter action flaps. [PR1622585](#)

General Routing

- The sensord: Error updating RRD file: /var/run/sensord.rrd error message might be generated on the WRL9 based line card. [PR1420927](#)
- 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 VC global switchover. [PR1518467](#)
- Junos 'et-' interface stuck and remains down between two particular ports. [PR1535078](#)
- The process grpcd might crash if flapping routes or interfaces. [PR1565255](#)
- MAC addresses might not be relearned successfully after MAC address age timeout. [PR1567723](#)
- When using log templates (introduced in 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](#)
- Packets with the MAC address of eth0 and macvlan0@eth0 interface might be sent out to the management interface on VMHOST platform with specific NG-RE. [PR1571753](#)
- The pkid process might occur during local certificate enrollment. [PR1573892](#)
- The chassisd process might crash on all Junos platforms that support Virtual Chassis. [PR1574669](#)
- The CHASSISD_FRU_IPC_WRITE_ERROR: fru_send_msg: FRU GNF 2, errno 40 error message might get generated periodically in the chassisd logs. [PR1576173](#)
- MIC specific alarms might not be cleared after MIC reboot. [PR1576370](#)
- The line cards might fail after hitting the I2C error on MX FPC. [PR1583060](#)
- A high rate of small packets could cause CPU hogging and firmware crash in MPC5E and MPC6E cards. [PR1587551](#)
- PEM capacity shows incorrectly on MX10003 platform. [PR1587694](#)
- NAT EIM mapping is getting created even for out to in FTP ALG child sessions. [PR1587849](#)
- Fabric link training could be seen if fabric self ping silently discards traffic. [PR1590054](#)
- Some IFLs might go down under logical tunnel due to the limited number of mac addresses in a pool. [PR1591853](#)

- The DCI InterVNI and IntraVNI traffic might black-holed in gateway node due to the tagged underlay interfaces. [PR1596462](#)
- The I2alm fails to send IPC message to the I2ald which may cause the FPC to crash. [PR1596615](#)
- EVPN-VXLAN shared tunnel knobs need to be removed. [PR1598142](#)
- The mspmand daemon memory leak might be observed after the HA master goes down. [PR1598356](#)
- The I2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable. [PR1599094](#)
- Traffic might get silently discarded upon link flap after a topology change. [PR1599215](#)
- The gNMI Telemetry might stop working after the Routing Engine switchovers. [PR1600412](#)
- Ipv6 link local BFD session might not come up if we dont have child link of an ae mapped to pfe inst 0. [PR1602493](#)
- Jflow-syslog for CGNAT might use 0x0000 in IPV4 Identification field for all fragments. [PR1602528](#)
- When using J-Web with HTTP an attacker may retrieve encryption keys via Person-in-the-Middle attacks. [PR1603199](#)
- 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](#)
- Traffic loss might occur on the device due to the continuous errors happening on Fabric Healing process (FHP) phase-1. [PR1603499](#)
- VRRP and BFD might flap on IRB interface on MPC10/11 line cards. [PR1604150](#)
- NPC logs seen when vrf localisation is enabled. [PR1604304](#)
- Traceroute status is unhelpful sometimes. [PR1604317](#)
- GRE tunnel might flap when hierarchical-scheduling configured. [PR1605189](#)
- The interface on MCP3-NG HQoS/MPC7E flaps continuously after enabling LACP on AE interface. [PR1605446](#)
- VM host platforms might boot exactly 30 minutes after executing the request `vmhost halt` command. [PR1605971](#)
- 5G-CUPS:bbe-cups-5G-setup:wf-eabu-dev.tadcaster:re1 {version} vmcore.0.gz. [PR1606146](#)
- Observing continuous SNMP trap for "Over Temperature!" for all the Renault_Daniel line cards. [PR1606555](#)

- Random IP assignment might be done on MX platforms configured with PCP and DS-Lite. [PR1606687](#)
- 'WO-0: OGE0 dequeue watermark hit' might be seen with L2 related configuration and receiving jumbo-frame packets. [PR1606967](#)
- 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 platforms. [PR1607077](#)
- TCP traffic might be dropped on source port range 512 to 767 when the FlowSpec IPv6 filter is configured. [PR1607185](#)
- The speed auto-negotiated SFP-T transceiver might not be joined to the AE after performing dcd restart or RE switchover on MX104. [PR1607734](#)
- The FPC might crash when the option 'sensor-based-stats' is configured. [PR1608871](#)
- On MX204 platform cannot successfully upgrade to Junos OS Release 21.2R2 image. [PR1609377](#)
- 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](#)
- On MX204 device, interface flaps might be observed on certain ports. [PR1609988](#)
- 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 due to one way congestion. [PR1611091](#)
- Erratic behaviour might be seen on platforms using MPC line cards after ISSU is performed. [PR1611165](#)
- Inter-vlan connectivity might be lost in an EVPN-VXLAN with CRB topology. [PR1611488](#)
- Duplicate value of add path IDs observed when the telemetry export is done for routes under BGP or for ext-attributes under BGP. [PR1612067](#)
- The routing protocol engine CPU is getting stuck at 100 percentage. [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](#)

- Memory might be exhausted when both the BGP rib-sharding and the BGP ORR (Optimal Route Reflection) enabled. [PR1613104](#)
- Traffic loss might be observed due to the shaping rate be adjusted incorrectly in a subscriber environment on MX platforms. [PR1613126](#)
- Enhanced-hash-key might not take effect when configured with forwarding-options. [PR1613142](#)
- IGP routing updates might be delayed to program in PFE after interface flaps in a scaled BGP routes environment. [PR1613160](#)
- For PS Service IFL configured in MPC2-NG/MPC3-NG interface stats do not show correct (shaped) value when shaping is applied. [PR1613395](#)
- Enabling security-metadata-streaming DNS policy may cause a dataplane memory leak. [PR1613489](#)
- The process rpd might crash in BGP rib-sharding scenario. [PR1613723](#)
- Any irrelevant configuration changes may trigger NAT routes flap on MX in USF mode. [PR1614688](#)
- MPC6E 3D did not comes back up after MIC offline online test. [PR1614816](#)
- Modifying the input service-filter via COA might fail in subscriber management environment. [PR1614903](#)
- Line-cards might be unstable due to 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 EVPN scenario. [PR1615269](#)
- Traffic drop might occur when huge number of EIM mappings are created/deleted continuously. [PR1615332](#)
- Request to provide an api which gives list of potential policy given a session id. [PR1615355](#)
- rasdaemon 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](#)
- The show subscribers accounting-statistics and show services l2tp session interface asi0.xx statistics commands might not work on LNS with asi- interfaces. [PR1616454](#)
- The dual Routing Engine system might not be GRES ready after backup RE reboot in a subscriber management environment. [PR1616611](#)

- ICMP error packet does not have relevant header when configured with DSLite and with appropriate ICMP ALG name and one UDP application name. [PR1616633](#)
- L2 cpd memory leak might lead to l2cpd process crash. [PR1617151](#)
- MPC8E in 1.6T bandwidth mode may not work correctly. [PR1617469](#)
- The l2cpd core 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 sent out 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 platforms 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 be stuck during rebooting the one redundancy line-card of RLT. [PR1620227](#)
- On MX480 device, 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](#)
- IFLSet COS hierarchy might be missed in the backup leg after rebooting FPC. [PR1621164](#)

- Flapping of all ports in the same PFE may cause PFE to be disabled. [PR1621286](#)
- Commit failure while applying tunnel interface configs using openconfig CLI. [PR1621369](#)
- Traffic loss can be seen on the new master RE post GRES. [PR1621696](#)
- FPC crash when macsec interfaces configured with bounded delay feature is deleted. [PR1621868](#)
- 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](#)
- [G.8275.1]: High phase jump spikes of ~4000 to 5000 ns is observed during slave clock fail-over within same line card, due to config commit. [PR1622575](#)
- Constant increase of PCS errors may be seen on channelized port. [PR1622741](#)
- Port speed might show as 100G even though chassis configuration is set for 40G manually. [PR1623237](#)
- chassisd memory leak may be seen after adding or removing an interface configuration. [PR1623273](#)
- The aggregated Ethernet member link might not be correctly populated on the PFE after FPC restart on MX series platforms. [PR1624772](#)
- On single IPSec tunnel with PMI when sending internet traffic packet processing might get delayed due to session management issue. [PR1624974](#)
- Specific packets over VXLAN cause FPC reset. [PR1625292](#)
- The flowd process lost heartbeat for 45 consecutive seconds without alarm raised. [PR1625579](#)
- 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 platform with SPC3 line card. [PR1625888](#)
- The bbe-smgd might crash on backup RE after ISSU/GRES. [PR1626091](#)
- Some Interfaces might not come online after linecard reboot. [PR1626130](#)
- Implement the show task scheduler-slip-history command 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 option 80 (rapid commit) ahead of option 82. [PR1626558](#)
- 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](#)
- Memory leak may occur on PFED process when the flat-file-profile is configured with knob 'use-fc-ingress-stats'. [PR1628139](#)
- EAPoL packets over I2circuit may get dropped at the tunnel start. [PR1628196](#)
- Tunnel-service bandwidth should not be changed when there are active subscribers. [PR1628628](#)
- The I2ald 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 every few minutes on MX platforms. [PR1630070](#)
- LLDP packets may be sent with incorrect source MAC for RETH/LAG child members. [PR1630886](#)
- The kmd might crash since the pkid requested memory leak happens on M/MX platforms. [PR1631443](#)
- ipv6 host route prefix match disappear from 'forwarding-table' after a ping test, ping continues to work, forwarding table entry is not shown. No impact in traffic. [PR1631607](#)
- 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](#)
- [CCL Google BX] RPD core 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 the aggregated Ethernet interface. [PR1633392](#)
- Slow chassis memory leak may occur when chassisd related configuration change is committed. [PR1634164](#)
- PTP clock class might incorrectly be downgraded to 248 when PTP is enabled on Linecard/MIC which does not support phy-timestamping. [PR1634569](#)
- CFM CCM PDU is not forwarded transparently on core MX if the ifd is configured under protocols oam. [PR1635293](#)

- Data might not be exchanged via EVPN-VxLAN domain. [PR1635347](#)
- Delay might be observed for the interfaces to come up after reboot/transceiver replacement. [PR1638045](#)
- Locally switched traffic might be dropped on ACX5448 with ESI configured. [PR1638386](#)
- On MX480 devices, PFED CPU increased post ISSU and remains around 65 to 75 percentage for 32,000 Layer 2 VPN sBNG services. [PR1643077](#)
- On MX104 devices, the request chassis afeb restart command returns timeout error. [PR1645322](#)
- Memory usage continuously increase is observed on backup chassis if subscriber service is enabled. [PR1595238](#)
- Commit related to dynamic profile configuration changes might fail upon executing the request vmhost reboot routing-engine both command. [PR1607494](#)
- DHCP subscribers might not be synchronized to backup BNG when DHCP ALQ is configured without topology-discover. [PR1620544](#)

High Availability (HA) and Resiliency

- Memory leaking might occur on the backup Routing Engine when ksyncd is in inconsistent state and had encountered an initialization error. [PR1601960](#)
- When MTU is configured on an interface a rare ifstate timing issue could occur at a later point resulting in ksyncd process crash on the backup Routing Engine. [PR1606779](#)

Interfaces and Chassis

- Duplicate source and destination pair check is done only across same tunnel encapsulation type for FTI. [PR1599266](#)
- On MX960 device, DAEMON-5: lo0 family maximum labels is non-adjustable in syslog messages. [PR1611098](#)
- Commit check failure may happen if similar interfaces are configured under VRRP group. [PR1617020](#)
- Delay in application of CLI configuration by DCD when ae interface members are configured via JET API. [PR1621482](#)
- The subscribers might be deleted when the host-prefix-only statement is configured on the underlying-interface in GRES scenario. [PR1630229](#)
- The syslog messages and the dcd crash might occur. [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% CPU utilization. [PR1636093](#)
- FPC might crash if the continuity-check interval under CFM is modified. [PR1636226](#)
- "show vrrp extensive" doesn't show the next IFL "Interface VRRP PDU statistics". [PR1637735](#)
- The ae interface with 400GE gets flapped on adding/removing a 400GE member link. [PR1641585](#)
- The vrrpd core might be observed after interface state change. [PR1646480](#)

Juniper Extension Toolkit (JET)

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

Junos Fusion Provider Edge

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

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](#)
- BFD hold-down timer doesn't work properly when LAG is configured. [PR1616764](#)
- Enabling DHCP on Junos and Junos Evo platforms might cause the router's file system storage to get filled up with log files. [PR1617695](#)
- The jdncpd crashes upon receiving a specific DHCP packet. [PR1618977](#)
- Circuit-id handled incorrectly with backup node for ALQ with Topology discover configured. [PR1620461](#)
- The jdncpd process crashes in DHCP/DHCPv6 environment. [PR1625011](#)
- The process jdncpd may get stuck at 100% 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

- The node SID might be seen in an unresolved state. [PR1564169](#)
- LDP P2MP traffic may be interrupted post GRES. [PR1609559](#)
- LDP does not support policy import with rib-groups. [PR1611081](#)
- The process rpd might crash if express segments using SR-TE underlay are configured. [PR1613372](#)
- The rpd core dumps might occur for few value configurations of signaling bandwidth on container LSP. [PR1614248](#)
- Protected LSP goes down with strict hops and link protection configured. [PR1616841](#)
- LDP protection paths might not be established when the auto-targeted-session command is deactivated and activated. [PR1620262](#)
- The rpd memory leak might 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](#)
- Rtsdbd core might be seen when IPsec configuration is activated and deactivated. [PR1610594](#)
- 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. [PR1613874](#)

Platform and Infrastructure

- FPC crash might be seen in firewall filter scenario. [PR1589619](#)
- XMCHIP_CMERROR_PT_INT_REG_PCT_PAR_ERR (0x70296) might be observed on MPC5 card which triggers PFE 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 platforms vmcore on both the routing engines might be reported due to mbuf corruption. [PR1602442](#)
- The FPC might crash if 'flow-table-size' is configured on MX platforms. [PR1606731](#)
- 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 very high PPS rate traffic. [PR1619111](#)
- CoS custom classifier might not work on logical interface. [PR1619630](#)
- Trio-based line cards might crash when PFE memory is hot-banking. [PR1626041](#)
- Configuration commit may fail while configuring the knob 'authentication-key-chains' under groups. [PR1626400](#)
- Unrealistic service accounting statistics might be reported due to firewall counter corruption. [PR1627908](#)
- The gencfg_cfg_msg_gen_handler drop error message might be seen after running commit command. [PR1629647](#)
- The packet drop might be seen on FPC on Trio based platforms. [PR1631313](#)
- When route preferred-metric is different for different RPM policies, the same metric is not reflected in routing records. [PR1634129](#)
- Continuous Fabric Link Sanity Check interrupts in intervals of weeks might cause at some point fabric input block traffic silently discard. [PR1636060](#)
- The vmxt_lnx core found at topo_get_link_jnh_features_get_jnh_jnh_stream_attach. [PR1638166](#)

Routing Policy and Firewall Filters

- BGP import policy is not applied to all the routes when CCNH inet is enabled. [PR1596436](#)

- Evaluation of inet-vpn route-filters might not work with /32 exact statements for BGP flowspec routes. [PR1618726](#)

Routing Protocols

- The rpd process might crash in a corner case in PIM-SM scenarios. [PR1574731](#)
- The rpd might crash in BGP multipath scenario if interface for a single hop EBGP peer goes down. [PR1589141](#)
- The process rpd might crash post GRES. [PR1590912](#)
- Observing commit error while configuring "routing-options rib inet6.0 static" on all Junos platforms. [PR1599273](#)
- The rpd core might be observed due to memory corruption. [PR1599751](#)
- Kernel crash might be observed on platforms having BGP configured with family Layer 2 VPN. [PR1600599](#)
- rpd crash might be seen after deactivating/activating interfaces. [PR1605620](#)
- The BGP replication may be stuck in InProgress state. [PR1606420](#)
- Multicast traffic might be duplicated on subscriber interface on MX platforms. [PR1607493](#)
- The rpd may 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](#)
- 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](#)
- The rpd may 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](#)
- The BFD session might be down when multiple addresses of same subnet are configured. [PR1635700](#)

Services Applications

- L2TP tunnels may 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](#)
- DTCP radius-flow-tap fails to program PFE when trigger X-NAS-Port-Id exceeds 48 character length. [PR1647179](#)

Subscriber Access Management

- Prefix duplication errors might occur for DHCPv6 over PPPoE subscribers. [PR1609403](#)
- Class attribute is corrupted for Radius accounting messages since ISSU to 19.1 or higher release on MX series platforms. [PR1624066](#)
- Radius CoA (Change of Authorization) NAK may not be sent with the configured Source Address in a virtual-router environment. [PR1625858](#)

- ESSM sessions may get terminated in Radius as class attribute has got corrupted after performing ISSU. [PR1626718](#)
- Event-timestamp in radius Acct-Stop may show future time. [PR1643316](#)

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](#)
- The core files can not be deleted using CLI "file delete /var/core/*/vmcore*". [PR1624562](#)
- Junos upgrade may fail with error "configuration database size limit exceeded". [PR1626721](#)

VPNs

- The multicast route is not getting installed after exporting of secondary routes from one instance to another. [PR1562056](#)
- Wrong st0 IFL deletion at spoke when multiple VPNs negotiate same destination address as TS. [PR1601047](#)
- The rpd process might crash during ISSU if the auto-sensing knob is enabled for I2circuit. [PR1626219](#)

Resolved Issues: 21.2R2

IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 180](#)
- [Class of Service \(CoS\) | 180](#)
- [EVPN | 180](#)
- [Forwarding and Sampling | 181](#)
- [General Routing | 181](#)
- [High Availability \(HA\) and Resiliency | 189](#)
- [Infrastructure | 189](#)
- [Interfaces and Chassis | 189](#)
- [J-Web | 189](#)
- [Junos Fusion Enterprise | 190](#)

- Layer 2 Ethernet Services | 190
- MPLS | 190
- Network Address Translation (NAT) | 191
- Network Management and Monitoring | 191
- Platform and Infrastructure | 191
- Routing Policy and Firewall Filters | 192
- Routing Protocols | 192
- Services Applications | 193
- Subscriber Access Management | 193
- User Interface and Configuration | 194
- VPNs | 194

Application Layer Gateways (ALGs)

- The ALG traffic might be dropped. [PR1598017](#)

Class of Service (CoS)

- Child mgd processes might become nonresponsive when multiple sessions continuously request for interface information. [PR1599024](#)
- Traffic loss might occur if you configure per-unit-scheduler on the aggregated Ethernet interface. [PR1599857](#)
- The 802.1p rewrite policies might not have any effect if you tie the rewrite to circuit cross-connect interfaces. [PR1603909](#)

EVPN

- Configuring static-mac and no-mac-learning simultaneously on the VXLAN interface causes stale MAC/IP entry in the EVPN database. [PR1576147](#)
- Few ARP/ND/MAC entries for VLANs are missed with the MAC-VRF configuration. [PR1609322](#)
- Change in display of nexthop type for EVPN Type-5 route occurs. [PR1576421](#)
- The BUM traffic might be dropped after changing any configuration on the device without the configured router-id. [PR1576943](#)

- The BUM traffic might be lost after triggering NSR in the EVPN-MPLS or EVPN-ETREE scenario. [PR1586402](#)
- The traffic might be dropped when you resolve the EVPN and Layer 3 VPN routes using the same MPLS-over-UDP tunnel. [PR1587204](#)
- The traffic might be dropped in the EVPN-VXLAN multihomed scenario. [PR1590128](#)
- Traffic loss might occur under the EVPN-VXLAN scenario when MAC-IP moves from one CE interface to another. [PR1591264](#)
- Transit traffic gets dropped after you disable one of the PE-CE links on a remote multi-homed PE device in the EVPN-MPLS A-A setup with Dynamic-List NextHop configured. [PR1594326](#)
- EVPN might not work properly in the multi-homed setup. [PR1596723](#)
- The device announces router-MAC, target, and EVPN VXLAN community to the BGP IPv4 NLRI. [PR1600653](#)

Forwarding and Sampling

- Logical interface statistics for the aggregated sonet displays double value than expected. [PR1521223](#)
- The snmpwalk process might not get polled in the MIB for the dual-stack interface. [PR1601761](#)

General Routing

- Node name must not be attached to the system hostname under LLDP. [PR1593991](#)
- Memory usage continuously increase on the backup chassis if you enable the subscriber service. [PR1595238](#)
- The I2ald process might crash due to memory leakage when all active interfaces in a VLAN are unstable. [PR1599094](#)
- Local Privilege Escalation and Denial of Service appears. [PR1568654](#)
- Traffic might drop if MS-MPC/MS-PIC resources gets consumed by certain traffic, causing a partial DoS. [PR1582030](#)
- IGP routing updates might delayed to program in the Packet Forwarding Engine after the interface flaps in a scaled BGP routes environment. [PR1613160](#)
- The I2ald process might crash in the EVPN scenario. [PR1615269](#)
- Request to provide an API, which gives list of potential policy, gives a session ID. [PR1615355](#)

- The MPC8E line cards in the 1.6T bandwidth mode might not work correctly. [PR1617469](#)
- With the scaled IPv6 synced sessions, clearing sessions on the primary MX router and stateful synchronization do not clear all the NAT64 sessions on the backup MX router. [PR1618360](#)
- Support for whole (atomic) updates at CNHG level occurs. [PR1619011](#)
- The nsd process generates core files while validating the NAT translation with the configured NAT44. [PR1619216](#)
- EVPN Type 5 routes might not be installed. [PR1620808](#)
- Commit failure with the error: load failure on translation changes syntax error gets generated while applying tunnel interface configurations using the openconfig cli command. [PR1621369](#)
- Enabling security-metadata-streaming DNS policy might cause a dataplane memory leakage. [PR1613489](#)
- A vulnerability in the Juniper Agile License Client might allow an attacker to perform the Remote Code Execution. [PR1582419](#)
- On MX480 routers, the subinfo process generates core file with the Layer 2 Node Scaling. [PR1598187](#)
- SSL-FP logging for non SNI session occurs. [PR1442391](#)
- Inaccurate allocated memory for nh and dfw_rulemask under kernel might occur. [PR1475478](#)
- The 40G or 100G interfaces might flap during ISSU if you deactivate PTP on the interfaces. [PR1546704](#)
- The interface might not come up with 1G optics. [PR1554098](#)
- Some transmitting packets might get dropped due to the disable-pfe action not being invoked when the fabric self-ping failure occurs. [PR1558899](#)
- On the MPC10E line cards, the interface is unable to send or receive packets after repeated flapping of the 100G link. [PR1560772](#)
- The MX150 router might reboot after you commit the request system snapshot recovery command. [PR1565138](#)
- The show pfe statistics traffic command displays incorrect output. [PR1566065](#)
- When you use the log templates (introduced in Junos OS Release 21.1R1) with unified policies, logs are not generated in a predictable manner. [PR1570105](#)
- PDB pull or synchronization might fail during unified ISSU. [PR1570841](#)

- High CPU usage might occur on RPD for routes that use the static subscriber. [PR1572130](#)
- Some MPC4E-3D- displays si5374 clock PLL lock timed out error message at boot up. [PR1573729](#)
- Only root user can execute commands on the host using vhclicent. [PR1574240](#)
- DS-Lite throughput degradation might occur on MS-MPC. [PR1574321](#)
- Configuration of child inactivity-timeout under custom ALG configuration does not take effect. [PR1575183](#)
- IPsec tunnel does not get established while receiving the proxy-id list. [PR1576071](#)
- On MX10016 routers, when the Fan X Failed alarm gets cleared in the Fan Tray 1, the Fan/Blower OK SNMP traps gets generated for the Fan Tray 0 [Fan 31 - 41] and Fan Tray 1 [Fan 11 - 41]. [PR1576521](#)
- The MPC7E, MPC10E, MX-SPC3 and LC2103 line cards might become offline when the device runs on the FIPS mode. [PR1576577](#)
- Mirrored packets get corrupted when you apply filter with port-mirror action and discard. [PR1576914](#)
- The MPC7E, MPC8E, MPC9E, and MPC11E line cards might become nonresponsive in the Unresponsive state in a Junos Node Slicing setup. [PR1580168](#)
- vmcore might occur after adding or deleting the logical interface of the static interface in the Next Generation Subscriber Management subscriber scenario. [PR1581260](#)
- Communication between two CE devices might fail when you enable the BGP rib-sharding. [PR1582210](#)
- The rpd process might become nonresponsive in the race condition. [PR1582226](#)
- Traffic drop might occur with SPC3 in the DS-LITE scenario. [PR1582447](#)
- USB boot with image gets stuck and does not boot the device. [PR1582592](#)
- Load balancing does not work correctly on the AMS interfaces for CGNAT traffic on the MX USF mode with SPC3. [PR1582764](#)
- On MX150 router, the bcmd process might crash. [PR1583281](#)
- Layer 2 multicast VXLAN instance goes down as the local vtep logical interface does not get associated to the EVPN instance. [PR1584109](#)
- Secure Web proxy continues to send the DNS query for the unresolved DNS entry even after removing the entry. [PR1585542](#)
- Traffic drop after enable the flexible-queuing-mode on the MPC2E line cards. [PR1586403](#)

- The RPD_KRT_KERNEL_BAD_ROUTE error message might occur on certain scenarios when the rpd process restarts or GRES occurs when you enable NSR that has no functional impact. [PR1586466](#)
- The bbe-smgd process might crash if the staled ACI-based subscribers do not clean up properly. [PR1587792](#)
- The na-grpc process might crash and existing telemetry connections might get disconnected. [PR1587956](#)
- 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 login or login of the subscribers. [PR1589081](#)
- The jsd process might crash in a rare condition in a telemetry scenario. [PR1589103](#)
- Traffic loss might occur for interface configured in the subnet 137.63.0.0/16. [PR1590040](#)
- Fabric link training occurs if the fabric selfping silently discards traffic. [PR1590054](#)
- The VXLAN DDoS violation might occur when you disable the port mirror analyzer output interface. [PR1590150](#)
- Even before the FPC or SLC comes online fully during the phase 2 of fabric healing and fabric healing reports, the restart-action is completed. [PR1590335](#)
- Traffic loss might occur 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 the AMS switchovers and, deactivating or activating the NAT service. [PR1590890](#)
- Traffic loss might occur after you change the SAK keys. [PR1591432](#)
- If you configure the COS CR-features used by VBF service, MPC might crash with subscriber. [PR1591533](#)
- PTP synchronization might get unstable. [PR1591667](#)
- The clear-ipsec-sas-for-duplicate-ts does not clear the Secure Access (SA) for duplicate traffic-selectors (TS). [PR1591735](#)
- xSTP might not get configured when enabled on an interface with SP style configuration. [PR1592264](#)
- The aftmand process might crash when you configure an interface with analyzer. [PR1592267](#)

- The mobiled daemon might crash after switchover for an AMS interface or might crash on the service PIC where the AMS member interfaces are present. [PR1592345](#)
- AMS warm standby with deterministic NAT functionality might not work properly. [PR1592437](#)
- Routing Engine kernel might crash due to logical interface of the aggregated Ethernet interface adding failure in the Junos kernel. [PR1592456](#)
- The l2cpd-agent might become nonresponsive after starting the telemetry service. [PR1592473](#)
- Using the BITS interface from the backup Routing Engine for the 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 the occurrence of the shared memory queues issue in a rare condition. [PR1592889](#)
- The TCP connections to the telemetry server might become nonresponsive in the CLOSE_WAIT status. [PR1593113](#)
- The TCP keepalive might not be processed by the private network host. [PR1593226](#)
- The IPv6 neighbor might remain unreachable in VRRP for IPv6 scenario. [PR1593539](#)
- Jweb deny log nested-application displays as UNKNOWN instead of the specific application. [PR1593560](#)
- Fabric errors get generated after swapping the MPC10E line card with MPC7E line card in the same slot. [PR1593821](#)
- The dcpfe process might crash in the EVPN-VXLAN scenario. [PR1593950](#)
- Packet might be dropped when the traffic moves from one FPC to another FPC. [PR1594244](#)
- The label field for the EVPN Type 1 route is set to 1. [PR1594981](#)
- The MX5, MX40, and MX80 router TEB becomes nonresponsive in the present state. [PR1595107](#)
- The interface down might be delayed after you commit the `set interface interface_name disable` command. [PR1595682](#)
- Firmware might fail to be downloaded to MIC on the MX Virtual Chassis setup. [PR1595693](#)
- Mismatch in the primary and backup Routing Engines with inetcolour tables and BGP-SRTE tunnels, after rpd-restart on primary occurs. [PR1596095](#)
- The Packet Forwarding Engine wedge might occur if you receive many IPv4 packets that need to be fragmented. [PR1596100](#)

- The l2ald process might crash on all leaves and spines after adding a new leaf to the EVPN fabric. [PR1596229](#)
- The DCI interVNI and intraVNI traffic might silently discard traffic in the gateway node due to the tagged underlay interfaces. [PR1596462](#)
- The mcsnoopd process might crash during the deletion or addition of the layer-2 forwarding configuration after ISSU. [PR1596483](#)
- The USF-NSD process generates core file while verifying the session-limit rate if you apply the bypass-traffic-on-exceeding-flow-limits command properly. [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](#)
- The bbesmgd process generates core file after the Routing Engine goes down. [PR1596848](#)
- Traffic fails to recover after multiple quick dot1xd restarts when you enable the MACsec suspend-for. [PR1596854](#)
- CGNAT MX SPC3 AMS warm-standby 1:1 redundancy problem occurs with the CLI CPU statistics lost data after the PIC failover. [PR1596976](#)
- Major alarms on all FPCs in chassis might occur after some time from bootup. [PR1597066](#)
- The screen drops statistic does not increment when you test the session limits by destination with max sessions configured. [PR1597382](#)
- The MAC/IP withdraw route might be suppressed by RPD in the EVPN-VXLAN scenario. [PR1597391](#)
- On MX10016 router, the Plane not online SFB alarm gets generated after the primary Routing Engine switchovers. [PR1597630](#)
- Deletion of the MACsec configuration on the logical interface does not take effect. [PR1597848](#)
- Subscriber management daemons might continuously generate core files and shutdown with the Routing Engine sensors invalid configured. [PR1598351](#)
- The AFEB process might crash with MIC-3D-8DS3-E3. [PR1598411](#)
- Packet loop might occur after you receive the PCP request packets, which are destined to the software concentrator address. [PR1598720](#)
- Component sensor does not export logs for /components/component[name='Chassis']/state/description. [PR1598816](#)

- NSR switchover with BGP SR-TE tunnels might lead to the rpd process generating a core file. [PR1599446](#)
- The MX SPC3 applications for protocol ICMP does not get detected and does not allow user to modify the 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 received TCP ACK packet as a reply to the self-generated TCP keepalive. [PR1600619](#)
- The Duplicate Address Detection(DAD) flags occurs for the IRB interfaces after configuration of the removal and restoration that might lead to traffic blockage. [PR1601065](#)
- The BBE-SMGD process generates core file 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](#)
- Traffic might be dropped at the NAT gateway if you enable EIM. [PR1601890](#)
- A few line cards might not come up online with the increased-bandwidth mode. [PR1602080](#)
- Jflow-syslog for CGNAT might use 0x0000 in the IPv4 Identification field for all fragments. [PR1602528](#)
- The Packet Forwarding Engine might be disabled by a detected major CMERROR event while ungracefully removing the MIC from MPC2E-3D-NG/MPC3E--3D-NG. [PR1602939](#)
- Packet loss might occur on the filter-based GRE deployments. [PR1603453](#)
- The core-usf-qnc-a-fpc3.pic1-flwd_spc3.elf.0.tgz message appears while verifying the TCP-based logging functionality with GRES with the AMS-NextHop style. [PR1603466](#)
- NSSU with MACsec configuration might result in the fxpc process, generating a core file. [PR1603602](#)
- The npc process generates a core file while testing second CE-FACING FPC behavior in a non-localization change. [PR1604304](#)
- On MX150 routers, interface hold-time up does not work. [PR1604554](#)
- The interface on the MCP3-NG HQoS and MPC7E line card flaps continuously after you enable LACP on the aggregated Ethernet interface. [PR1605446](#)
- The MPLS transit router might push an extra Entropy label to the LSP. [PR1605865](#)
- Continuous Over Temperature! SNMP trap for all the Renault_Daniel line cards occurs. [PR1606555](#)

- 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](#)
- On MX104 router, the negotiated speed for an SFP-T interface does not get displayed after the interface-control daemon restarts or switchover. [PR1607734](#)
- Memory might leak on the l2cpd process when you perform certain LLDP operations. [PR1608699](#)
- The single-vlan tagged subscribers might fail to reconnect through dynamic-vlan over the PS interface. [PR1609844](#)
- When you use J-Web with HTTP, an attacker might retrieve encryption keys through the Person-in-the-Middle attacks. [PR1603199](#)
- Multicast streams might stop flooding in the VXLAN setup. [PR1606256](#)
- The authd process and RADIUS might have stale L2BSA subscriber entries. [PR1610476](#)
- The service PICs are unable to come up when you configure the dnsf package. [PR1612316](#)
- DS-Lite does not work and NAT rule lookup fails. [PR1612555](#)
- The l2ald process generates core file during routing-instance configuration change. [PR1612738](#)
- Memory might be exhausted when you use both the BGP rib-sharding and BGP ORR. [PR1613104](#)
- Traffic loss might occur due to the shaping rate being adjusted incorrectly in a subscriber environment. [PR1613126](#)
- Line cards might be unstable due to the continuous growth of the memory usage. [PR1614952](#)
- The show subscribers accounting-statistics and show services l2tp session interface asi0.xx statistics might not work on LNS with the asi- interfaces. [PR1616454](#)
- Reboot of the backup Routing Engine in a high-scaled subscriber management environment might result in the system not returning to a GRES ready state. [PR1616611](#)
- ICMP error messages do not get generated when the SFW and IPsec service-set are configured on single PIC. [PR1617830](#)
- The clksyncd process crashes with 1pps output and PTP/Hybrid gets configured by default post upgrade. [PR1618929](#)

High Availability (HA) and Resiliency

- When you configure MTU on an interface a rare ifstate timing issue could occur at a later point resulting in crashing of the ksyncd process on the backup Routing Engine. [PR1606779](#)

Infrastructure

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

Interfaces and Chassis

- Traffic might be interrupted when you add the xe or ge interfaces as a member of the aggregated Ethernet interface bundle. [PR1569399](#)
- ARP resolution failure might occur during VRRP failover. [PR1578126](#)
- JVISION optics sensor alarm data type changes from bool_val to str_val. [PR1580113](#)
- The dcd process might crash after the Routing Engine switchovers, reboots, or management interface configuration changes. [PR1587552](#)
- The dcd process might crash after removing the aggregated Ethernet child logical interface from the targeted distribution database. [PR1591032](#)
- Removal of the configuration from the interface stanza might cause the dcpfe process to crash. [PR1594356](#)
- The VRRP host cannot be reached if you configure the native-vlan-id. [PR1595896](#)
- The dcd process might crash and FPC might become nonresponsive in the Ready state. [PR1601566](#)
- The aggregated Ethernet interface might flap upon configuration changes. [PR1602656](#)
- Memory leak on the dcd process occurs when you commit configuration changes on any interfaces in a setup with the AMS interface configured. [PR1608281](#)

J-Web

- J-Web allows a locally authenticated attacker to escalate their privileges to root. [PR1592021](#)
- A path traversal vulnerability allows an authenticated attacker to elevate their privileges to root. [PR1591145](#)
- J-Web allows a locally authenticated attacker to escalate their privileges to root. [PR1594516](#)

Junos Fusion Enterprise

- Reverting mastership from the Routing Engine 1 to Routing Engine 0 might lead to crashing of the l2ald daemon and outage. [PR1601817](#)

Layer 2 Ethernet Services

- There is ALQ synchronization issue on the primary BNG and backup BNG with a loss of subscriber session redundancy through the PS interface. [PR1583310](#)
- The rpd process scheduler might continuously slip and slow commit after GRES when there are 7000 DHCP clients. [PR1625617](#)
- The subscriber login might fail on the backup BNG running ALQ and Redundancy Services does not become available. [PR1583445](#)
- The DHCP client might become offline for about 120 seconds after sending the DHCPINFORM message. [PR1587982](#)
- 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 generates core file in the backup Routing Engine at mirror_process_recvd_data_queue with 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 rpd process might crash with the LSP external controller configuration. [PR1601763](#)
- VPLS connection might get down if you configure the dual-transport command. [PR1601854](#)
- The RSVP detour LSP might fail to come up when an LSR in the detour path goes down. [PR1603613](#)
- The LDP P2MP traffic might be interrupted post GRES. [PR1609559](#)
- The rpd process might crash on the standby_re LDP module when you enable the VPLS mac-flush on peer by default or when you configure. [PR1610638](#)

Network Address Translation (NAT)

- The services NAT mappings and sessions get incorrectly displayed 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 appear. [PR1606600](#)

Platform and Infrastructure

- The process generates the HEAP malloc(0) detected! error message when you configure the adaptive load-balancing on a LAG. [PR1547240](#)
- Degraded traffic processing performance might be observed in case of processing very high PPS rate traffic [PR1619111](#)
- The fpc process might generate core files and might drop packet in the VXLAN-EVPN scenario. [PR1600030](#)
- Upon the 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 PPP or L2TP clients on si-0/4/0 and si-0/5/0 might get disconnected due to keep alive failure. [PR1570053](#)
- FPCs might crash randomly when you delete the interface-set in the system. [PR1571192](#)
- The traffic might not fail with shared-bandwidth-policer enabled on the aggregated Ethernet interface. [PR1588708](#)
- The audit process generates core file while changing the TACACs and login user passwords. [PR1589953](#)
- VLAN tagged traffic might be dropped with the service provider style configuration. [PR1598251](#)
- The service filter might be incorrectly programmed in the Packet Forwarding Engine due to a rare timing issue in the enhanced subscriber management environment. [PR1598830](#)
- The kernel might generate a core file if you restart the BGP connections after deleting the BGP authentication. [PR1601492](#)
- The ZTP service might not work and the image installation might fail. [PR1603227](#)

- The FPC might crash if you configure flow-table-size. [PR1606731](#)
- Multicast traffic gets dropped when forwarded over VPLS through IRB. [PR1607311](#)

Routing Policy and Firewall Filters

- The dns-name cannot be resolved if you configure the customer-defined routing instance under name-server. [PR1539980](#)

Routing Protocols

- The BGP session might be down due to BGP-LS TLV received out of order. [PR1546416](#)
- The rpd process generates core files upon the receipt of specific BGP update. [PR1595165](#)
- Incorrect authentication-algorithm gets set in the BGP neighbor. [PR1571705](#)
- After the first parallel ISSU, subsequent ISSU aborts with the Aborting Daemon Prepare message. [PR1572265](#)
- Short multicast packets drop using PIM when multicast traffic is received at a non-RPT/SPT interface. [PR1579452](#)
- The rpd process might crash in the BGP multipath scenario if the single hop EBGP peer goes down. [PR1585265](#)
- Traffic might drop and the link might flap if you configure IS-IS. [PR1585471](#)
- The rpd process might crash in the BGP multipath scenario if interface for a single hop EBGP peer goes down. [PR1589141](#)
- The rpd process might crash in a scaled routing instances scenario. [PR1590638](#)
- PIM joins might not be synchronized between the primary and backup Routing Engines because of the ppmmd process restart. [PR1591685](#)
- The rpd process might crash if the BGP peer flaps. [PR1592123](#)
- The remote LFA (loop-free-alternate) backup path might not be formed. [PR1592424](#)
- BGP Egress-TE routes lose to the BGP routes using the same protocol-preference. [PR1593332](#)
- The routing process might crash due to memory corruption while processing the BGP multipath route. [PR1594626](#)
- The NTF-AGENT process generates core file at Tthr_rwlock_unlock CRYPTO_THREAD_unlock OPENSSL_init_crypto. [PR1597714](#)

- IPv4 static route might still forward traffic unexpectedly even when the static route configuration has already been deleted. [PR1599084](#)
- Some routes might get incorrectly programmed in the forwarding table in the kernel with next-hop installed as DEAD. [PR1601163](#)
- The rpd process might become nonresponsive in the OSPFv3 scenario. [PR1601187](#)
- Packet might drop when you change the INET MTU for MPLS enabled interface in the IS-IS SPRING scenario. [PR1605376](#)
- On the MPC10E line card, the rpd process generates cores file at `rt_table_flash_job_cancel,rt_instance_set_lsi_ifl_data_shard,rt_flash_all_internal` deactivating or activating interfaces. [PR1605620](#)
- Multicast traffic might be duplicated on the subscriber interface. [PR1607493](#)
- With rib-sharding enabled, any commit flaps all the BGP sessions with 4 byte peer-as (AS number 65536 or greater). [PR1607777](#)

Services Applications

- 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

- Subscribers might become nonresponsive in the Terminated state when the RADIUS server becomes unreachable. [PR1600655](#)
- The Service session entry creation failed error message appears during the ephemeral commit. [PR1603030](#)
- Prefix duplication errors might occur for the DHCPv6 over PPPoE subscribers. [PR1609403](#)
- The DHCP session fails with the `session-limit-per-username` command. [PR1612196](#)

User Interface and Configuration

- The apply-path does not expand for the configuration under groups. [PR1592032](#)
- Invalid JSON and XML output format for the show system resource-monitor ifd-cos-queue-mapping fpc x | display [json|xml] command occurs. [PR1605897](#)

VPNs

- The rpd process might crash when you add or delete the link-protection from LSP for the MVPN ingress replication selective provider tunnel. [PR1469028](#)
- The iked process might crash when the IKEv2 negotiation fails. [PR1577484](#)
- Unable to add BGP standard community to the NGMVPN Type-6 and Type-7 routes in VRF export policy. [PR1589057](#)
- The packets failed the multicast RPF check DDoS-protection message might occur in the NG-MVPN scenario with the GRE transport. [PR1591228](#)
- The rpd process might crash if the interface goes down in the BGP-MVPN scenario. [PR1597387](#)

Resolved Issues: 21.2R1

IN THIS SECTION

- [General Routing | 195](#)
- [Class of Service \(CoS\) | 209](#)
- [EVPN | 209](#)
- [Forwarding and Sampling | 210](#)
- [General Routing | 210](#)
- [Infrastructure | 211](#)
- [Interfaces and Chassis | 211](#)
- [Intrusion Detection and Prevention \(IDP\) | 212](#)
- [J-Web | 212](#)
- [Juniper Extension Toolkit \(JET\) | 212](#)
- [Junos XML API and Scripting | 212](#)
- [Layer 2 Features | 212](#)
- [Layer 2 Ethernet Services | 213](#)

- MPLS | 213
- Multicast | 214
- Network Address Translation (NAT) | 214
- Network Management and Monitoring | 214
- Platform and Infrastructure | 214
- Routing Policy and Firewall Filters | 216
- Routing Protocols | 217
- Services Applications | 220
- Subscriber Access Management | 220
- User Interface and Configuration | 220
- Virtual Chassis | 221
- VPNs | 221

General Routing

- Revert of RLT to primary might silently discard traffic for around 10 minutes after the primary FPC is online with primary RLT up. [PR1394026](#)
- Unable to show to which shard a given route is hashed. [PR1430460](#)
- Configuring two IPsec gateways for V1 and V2, triggering IKEv1 client tunnels AutoVPN hub always checks with IKEv2 policy and not on IKEv1. [PR1465970](#)
- The following line card errors are seen: HALP-trinity_nh_dynamic_mcast_add_irb_topo:3520 snooping-error: invlaid IRB topo/ IRB ifl zero in l2 nh 40495 add IRB. [PR1472222](#)
- FPC might crash after performing unified ISSU on the device which equips the type of 3D 20x 1GE MIC. [PR1480212](#)
- Subscribing to /linecard/packet/usage and triggering the UDP decoder, the hardware statistics are exported with improper hierarchy. [PR1485739](#)
- Incorrect log message for PIC1 when changing the configuration from PIC mode to port mode. [PR1500429](#)
- Aggregate Ethernet interfaces do not display member link statistics. [PR1505596](#)
- MX150 routers might go into db mode after software upgrade or downgrade. [PR1510892](#)

- Sometimes external 1 pps cTE is slightly above Class B requirement of the ITU-T G.8273.2 specification. [PR1514066](#)
- On the MX960 routers, the `show interfaces redundancy rlt0` statement shows current status as primary down as FPC is still in the ready state after RLT failover (restart FPC). [PR1518543](#)
- Packet drops might be seen with all commit events when interface configured with 1 Gbps speed. [PR1524614](#)
- RADIUS framed route sent via RADIUS initiated COA message might not be installed into the routing table. [PR1524628](#)
- The aggregated Ethernet interface might not come up with LFM configured after reboot. [PR1526283](#)
- Removing superfluous XML tags within syslog strings. [PR1528116](#)
- On MX150 routers, configuring the `no-flow-control` statement under `gether-options` does not work. [PR1531983](#)
- Wavelength unlocked alarm is On when using SFP+-10G-T-DWDM-ZR optics. [PR1532593](#)
- On the Virtual Chassis and Virtual Chassis fan, after NSSU while performing GRES, backup can generate core file and go to the database prompt. [PR1533874](#)
- The `dcufe` process might crash and cause FPC to restart due to the traffic burst. [PR1534340](#)
- The CFM sessions go down during FRU upgrade stage of unified ISSU in MX Virtual Chassis. [PR1534628](#)
- The `spcd` process might crash during early initialization. [PR1535536](#)
- Certain Linux based FPCs might reboot if TNP neighbor towards backup Routing Engine continuously flaps on dual Routing Engine platforms. [PR1537869](#)
- The following error message might be seen during upgrade of VM host platform: `vmhost-platform-grub-install.sh: line 140: [: ==: unary operator expected`. [PR1537980](#)
- On the AFT based FPCs (MPC10 and MPC11 line cards), the `show jnh exceptions inst` command of the Packet Forwarding Engine might cause the FPC process to crash. [PR1538138](#)
- The BFD neighborhood fails with the EVPN VXLAN configuration after the Layer 2 learning restarts. [PR1538600](#)
- Configuration archival might not work. [PR1540843](#)
- The `dcufe` process might crash in the specific MAC move cases and traffic loss might be observed in the EVPN-VXLAN scenario. [PR1542709](#)
- The JNH memory leak could be observed on MPCs or MICs. [PR1542882](#)

- Sessions creation rate is set to minimal rate after IDS and CPU throttling in place during DDoS attack. [PR1544489](#)
- The kmd process might crash when the interface flaps. [PR1544800](#)
- The VM host platform might get crashed continuously after performing upgrade or downgrade and booting up with the new image. [PR1544875](#)
- The high priority queue might consistently drop traffic after SIB goes offline. [PR1545061](#)
- Continuous rpd process errors might be seen and new routes fails to be programmed by the rpd process. [PR1545463](#)
- FPC might not boot-up on MX960 routers in certain condition. [PR1545838](#)
- The 40G or 100G interfaces might flap during unified ISSU if PTP is deactivated on the interfaces on MX platforms. [PR1546704](#)
- OSPFv3 session might keep flapping and OSPFv3 hellos might be dropped in the host path. [PR1547032](#)
- The PTP protocol might get stuck at initializing state on MX platforms. [PR1547423](#)
- WR Linux 6 platforms and WR Linux 9 platforms might be stuck after upgrading or downgrading image version and restarting the device. [PR1547669](#)
- Traffic for some IPv4 over IPv6 entries is dropped. [PR1547681](#)
- SR-TE might stay in the Up state when the routes are deleted through policy. [PR1547933](#)
- MX platforms might stuck after performing vmhost reboot post image upgrade. [PR1548254](#)
- The MS-MPC and MS-MIC located at VC-B might not work properly in an MX Series Virtual Chassis. [PR1548340](#)
- Traffic with jumbo frame might be discarded on the vMX platforms. [PR1548422](#)
- FPC crash might occur after flapping the multicast traffic. [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](#)
- The firewall process crash might be seen if deactivating/activating the firewall during back to back switchovers. [PR1549856](#)
- PKI CMPv2 client certificate enrollment does not work when using root-CA. [PR1549954](#)
- The LLDP adjacency might not be established for fxp interface. [PR1550131](#)

- Error messages are observed as the backup peer does not send marker acknowledgment for the last 360 seconds for vks 0 slave_ack=0 during ISSU. [PR1550492](#)
- Two Routing Engines might lose communication if they have different Junos OS versions on MX10003 platforms. [PR1550594](#)
- The adapted sample rate might get reset to the configured sample rate without changing the sampling rate information in sFlow datagrams after enabling sFlow technology on a new interface. [PR1550603](#)
- Deleting or deactivating the PS interface must not be allowed when use by BBE subscriber. [PR1550915](#)
- Unintended FPC restarts might be seen on MX10008 and MX10016 routers due to small timeout value between line card and chassisd process. [PR1550917](#)
- Certain MX platforms might reset and fail to boot due to a failure accessing Solid State Drive (SSD). [PR1551047](#)
- Silent compact flash (/dev/ada1) failure might occur during reboot or startup of router. [PR1551171](#)
- The softwire might not be established when connecting to a different AFTR. [PR1552431](#)
- Firmware versions for MPC11E line card were not getting displayed due to the changes made to the API in software required to read the firmware versions from the hardware. [PR1552847](#)
- The interface might not come up with 1G optics. [PR1554098](#)
- Unified ISSU upgrade from pre Junos OS Release 19.1 to Junos OS Release 19.1 and later might cause a few interfaces to go down. [PR1554099](#)
- The following error messages seen when we issue CLI commands to fetch host route scale: Cattle-Prod Daemon received unknown trigger (type Semaphore, id 1). [PR1554140](#)
- CoS WRED Curve: Create Expr Curve: No curve data points!! error messages are seen when interpolate is configured under drop profile. [PR1554220](#)
- Global Ethernet flow-control should be disabled when PFC CNP is enabled on an interface. [PR1554345](#)
- The link on the Linux based LC is not brought down immediately after the FPC process(ukern/indus.elf) crashes or the process is killed. [PR1554430](#)
- On MX960 routers, SNMP index of output interface is reported as zero in the exported flow records of MPLS and MPLS-IPv4 sampling when ipv4 tunnel-observation statement is deleted on the fly. [PR1554489](#)

- The subscriber sessions might be missed but stay in the authd after performing unified ISSU. [PR1554539](#)
- The device takes 3-10 mins to bring up the 100-1000 subscribers. [PR1555216](#)
- The chassisd process might crash with repeated configuration commits on MX204 and MX10003 routers. [PR1555271](#)
- The VGA might be down when configuring the IRB interface with multi VGA addresses. [PR1555338](#)
- The subscriber's RADIUS interim accounting statistics update might not work in some scenario. [PR1555492](#)
- Fabric self ping failure might be reported from MPC10 line card when MPC CPU is busy. [PR1555802](#)
- The following message is not generated on the MPC11E line card due to no power: Chassisd SNMP trap Fru Offline. [PR1556090](#)
- FPC with power related faults might get on-lined again once fabric healing has off-lined the FPC. [PR1556558](#)
- The dcpfe process might crash and restart with a dcpfe core file created while running the Type 5 EVPN VXLAN with 2000 VLANs. [PR1556561](#)
- On the MPC9E line card, core file is generated when SFB is online after ISSU of a GNF. [PR1556627](#)
- The framed route installed for a demux interface has no MAC address. [PR1556980](#)
- Script fails while committing the IPsec authentication configuration as the algorithm statement is missing. [PR1557216](#)
- The framed-routes are stuck in KRT queued (pending) add state when the routing-service enable is configured under dynamic-profile. [PR1557230](#)
- Multiple FPCs crash might be seen when performing GRES or FPC reboot repeatedly in subscriber scenario. [PR1557294](#)
- Packets corruption on 100G or 40G when interface is configured with protocol PTP. [PR1557758](#)
- The MAC addresses learned in a Virtual Chassis might fail aging out in MAC scaling environment. [PR1558128](#)
- Application identity unknown packet capture utility does not function when enhanced-services mode is enabled. [PR1558812](#)
- Rpd process generates core file after Routing Engine switchover. [PR1558814](#)
- 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 device might run out of service post GRES or unified ISSU. [PR1558958](#)
- MX Series with MPC10 and MPC11 line card might crash and restart when traffic is hitting a firewall filter having a term with syslog action configured. [PR1559174](#)
- On MX150 routers, the following continuous license error is observed:
[licinfra_set_usage_nextgen_async:1733] Invalid input parameters. [PR1559361](#)
- The subscriber management infrastructure daemon (smid) process might be stuck at 100 percent. [PR1559402](#)
- Single rate three color policer does not work. [PR1559665](#)
- On MX960 routers, mismatch between YANG schema and RPC output are observed. [PR1559810](#)
- Zero suppression is disabled. [PR1559882](#)
- Untagged traffic routed over native-vlan might be dropped. [PR1560038](#)
- When the system has only one plane (in the process of plane offline or online), the MPC10-10C line card displays a destination error. [PR1560053](#)
- The PTP master line card servo might stuck in freerun state. [PR1560074](#)
- The jnxDomAlarmSet and jnxDomAlarmClear trap will be generated for a copper port. [PR1560149](#)
- The request system software validate command might corrupt installation of the junos-openconfig package. [PR1560234](#)
- The VXLAN queue DDoS violation and RARP packets flood might happen if receiving the RARP packets more than the supported DDoS bandwidth. [PR1560243](#)
- The PIC in SRX5K-SPC3/MX-SPC3 card might get stuck in offline status after flowd process crash occurs on it. [PR1560305](#)
- On MX240 routers, R0 overlay ping fails. [PR1560408](#)
- The class-of-service RED feature might work unexpectedly and cause traffic drop. [PR1560495](#)
- Telemetry might not work after reboot or upgrade. [PR1560496](#)
- Filters are not allowed on family any port-mirroring destination interface. [PR1560624](#)
- The FPC might reboot in a high-scale configuration scenario. [PR1560757](#)
- Interface does not able to send/receive packets after repeated link flaps on MPC10 and MPC11E line cards. [PR1560772](#)

- When LACP daemon is restarted, LACP local partner system id remains 0 in mc-ae output. [PR1560820](#)
- The native-vlan-id might not work as expected on MPC10E and MPC11E line cards. [PR1560849](#)
- FTP might fail when using in-band ports. [PR1561146](#)
- The tunable optics SFP+-10G-T-DWDM-ZR does not work. [PR1561181](#)
- SPC3 is not supported on MX in 21.1R1 for deployment. [PR1561188](#)
- The l2cpd process might generate core file on reboot. [PR1561235](#)
- The VIA headers might not be translated properly when the SIP ALG is enabled. [PR1561312](#)
- The CdaExprClient: grpc api call ExprServerInfoGet failed and CdaExprClient: Failed to fetch server info error:5 are seen on all FPCs after restarting router or FPC restart. [PR1561362](#)
- Firewall filters might not work after unified ISSU. [PR1561690](#)
- Traffic drop might occur on all platforms running Junos OS when a GRE-based dynamic tunnel is configured. [PR1561721](#)
- Unable to open configuration database during USB upgrading. [PR1561741](#)
- After recovering from restart routing immediately, object-info anomalies is observed on rpd agent. [PR1561812](#)
- Continuous bbe-smgd core files are generated after restarting the smgd. [PR1561855](#)
- Interface loopback might not work if there is no optics connected to the port. [PR1562471](#)
- The dcpfe process might crash after deleting VXLAN configuration. [PR1562692](#)
- LICENSE_INVALID_FEATURE_ID syslog message is not being logged. [PR1562700](#)
- Commit issue is seen after loading limited-signed image through USB. [PR1562723](#)
- The rpd process might crash when the routing-instances are deleted and recreated quickly. [PR1562905](#)
- FPC Online/Offline through pinhole is not working. [PR1563315](#)
- The AppID DB not erased after the request system zeroize command. [PR1563280](#)
- Client authentication is failing after performing GRES. [PR1563431](#)
- Routing Engine switchover on-disk-failure does not work as expected when GRES is disabled. [PR1563505](#)

- Layer 2 interface information is not included in DHCPv4 option-82 circuit-id/remote-id DHCPv6 relay-agent-interface-id/relay-agent-remote-id options when service provider style configuration for switch interfaces is employed. [PR1564010](#)
- It might take a long time to create physical interfaces after restarting the FPC. [PR1564156](#)
- The following error message might be seen after unified ISSU: Turbotx process not running. [PR1564418](#)
- MX platforms with MX-SCBE3 might reboot continuously. [PR1564539](#)
- Old template is found in p2mp rsvp LSPs after adding new template. [PR1564795](#)
- Upon receipt of specific packets, BFD sessions might flap due to DDoS policer implementation in Packet Forwarding Engine. [PR1564807](#)
- Commit error observed when tunnel-service is configured on a PIC without explicit bandwidth. [PR1565034](#)
- On MX2010 and MX2020 routers, the following error message might be observed after switchover with GRES/NSR: CHASSISD_IPC_FLUSH_ERROR. [PR1565223](#)
- Unable to bring up more than one client on one VLAN at the same time. [PR1565249](#)
- PPPoE service-name-tables does not correctly count active sessions that matches agent-specifier ACI/ARI used for delay. [PR1565258](#)
- The KRT log file might continue to grow after removing the KRT log configuration. [PR1565425](#)
- Core files are seen at grpc_slice_buffer_add_indexed with LSR core profile configuration. [PR1565427](#)
- The mspmand crash might be seen on the PIC of MS-MPC and MS-MIC. [PR1566325](#)
- LLDP does not work on the management interface. [PR1566454](#)
- Pushing more than 2 MPLS labels on might not work. [PR1566828](#)
- Rpd core files are generated at boot time of a device. [PR1567043](#)
- The chassisd crash might be seen on MX platforms. [PR1567479](#)
- TLB composite next hop is installed incorrectly in other routing-instances. [PR1567568](#)
- Need to allow the tunnel interface as the peer-address for ALQ. [PR1567735](#)
- On MX204 routers, FPC might display high CPU utilization because of the JGCI background thread that runs for a long period. [PR1567797](#)
- State is not established for the show bgp bmp station *name* after the authentication-key bmp-auth is configured. [PR1568046](#)

- MAC addresses might not be installed in the EVPN MAC table due to route churn. [PR1568130](#)
- Memory might be exhausted when BGP sessions are unstable. [PR1568551](#)
- BFD flaps might be seen between leaf and core during spine reboot causing other protocols flap. [PR1568615](#)
- SPC3 card interfaces are not created. [PR1568694](#)
- IPv6 ping not working, when the strict uRPF is enabled. [PR1568938](#)
- Traffic might be dropped when the default route is changed in inet.0 table. [PR1568944](#)
- The scu-class-name statement is taking more than 60 seconds to come up with scaled aggregated Ethernet configuration. [PR1568957](#)
- The nsd process might crash after turning off the address translation for the NAT rules in the USF scenario. [PR1568997](#)
- The rpd process might crash while using BFD API to bring up the BFD sessions. [PR1569040](#)
- Traffic loss might be observed when SCU accounting is configured and logical-systems is enabled. [PR1569047](#)
- The agent sensor __default_fabric_sensor__ are partly applied to some FPCs, which causes zero payload issue. [PR1569167](#)
- LLDP out-of-bounds read vulnerability in l2cpd. [PR1569312](#)
- Wi-Fi mPIM is reaching out to NTP and DNS servers. [PR1569680](#)
- The MPLS traffic passed through the back-to-back PE topology might match the incorrect CoS queue. [PR1569715](#)
- On MPC10 line cards, resolve to hold nh:776 not found in the database. [PR1569829](#)
- The mspmand process might crash if the packet flow-control issue occurs on MS-MPC and MS-MIC. [PR1569894](#)
- The log message /tmp//mpci_info: No such file or directory :error[1] might be seen on VM host platform. [PR1570135](#)
- The jinsightd process might be stuck with high CPU process utilization. [PR1570526](#)
- The bbe-smgd process might crash after committing several thousand addresses in a filter term. [PR1570536](#)
- The ZTP state machine might be stuck on the management interface for about 12 minutes. [PR1570598](#)

- Cleanup does not happen properly for subscribers stacked over static demux interface. [PR1570739](#)
- Upgrading with unified SSDs (2x32G SSD) might result in boot loop in certain scenario. [PR1571275](#)
- Packet loss might be observed when sample based action is used in firewall filter. [PR1571399](#)
- FPC crash might be seen when deleting a lot of multicast groups at the same time. [PR1571890](#)
- Switchover to backup Routing Engine if rpd was NSR ready and then crashed. [PR1571914](#)
- The gRPC session hanging in CLOSED state. [PR1571999](#)
- The grpcd process might crash and telemetry subscription will retry until grpcd restarts. [PR1572107](#)
- In transit spine devices, 100 percent DCI traffic loss is observed. [PR1572238](#)
- The TFEB/FPC might fail to be online after rebooting the system or the FPC if the interface-set is configured for CoS. [PR1572348](#)
- Segment routing might not work properly in IS-IS multiple levels setup. [PR1572391](#)
- The show services mobile-edge sessions summary access-network-peers command displays incorrect established subscriber output after the UPF handover ENB step. [PR1572520](#)
- On MX960 routers, the Require a Fan Tray upgrade alarm is raised when the top Fan Tray 0 is removed, even though the enhanced Fan Tray is already used. [PR1572778](#)
- A traffic loop might be observed after the VCP interface flap. [PR1573047](#)
- CFP unplugged message is not logged. [PR1573209](#)
- Fabric errors are observed and FPC processes might get offline when MPC3-NG or MPC3E line cards are installed along with MPC7/MPC10 and SCBE3/SCB4 operating in increased-bandwidth fabric mode. [PR1573360](#)
- The rpd process on the transit node might crash when MPLS traceroute on the ingress node is performed. [PR1573517](#)
- ARP traffic exceeding the policer limit is not discarded. [PR1573956](#)
- QSFP 4x10G interface might not come up after FPC reboot. [PR1574279](#)
- DS-Lite throughput degradation might be seen on MS-MPC. [PR1574321](#)
- Slow FPC heap memory leak might be triggered by flapping the subscribers terminated over multiple pseudowires. [PR1574383](#)
- The mpls-template for J-Flow version 9 cannot make a similar template to mpls-ipv4-template on MX MS-MIC/MPC. [PR1574402](#)

- PIM rib-group fails to be added in VRF. [PR1574497](#)
- On the EA-based cards IGMP group membership is displayed incorrectly. [PR1575031](#)
- PTP might be stuck in Phase acquiring state after ISSU upgrade [PR1575055](#)
- The rpd process might continuously crash if deleting forwarding-class policy with discard action. [PR1575177](#)
- 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 the MX150 routers, the interface might take a long time to power down while rebooting, powering-off, halting, or upgrading. [PR1575328](#)
- 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_recv_ 1237: ipc_pipe_read fails! error:No error: 0(0), tries:1. [PR1576044](#)
- MPC crash might be seen when the next-ip action is used for filter-based forwarding. [PR1576695](#)
- The LLDP neighbor information displays hex string instead of chassis ID when subtype 1 is used. [PR1576721](#)
- The MS-MPC and SPC3 might reset on receiving the subscriber traffic. [PR1576946](#)
- Traffic drop and the aftd process crash are seen on MPC10 line card. [PR1576997](#)
- The following commit failure-error is observed: Modified IFD "ae0" is in use by targeted BBE subscriber, commit denied - mtu config changed (1522), (1514). [PR1577007](#)
- Traffic loss might be seen when subscriber service over aggregated Ethernet bundle interface. [PR1577289](#)
- Object anomalies are seen with PTP TC configuration. [PR1577375](#)
- When line card is booted on Routing Engine 1 being master, Next-gen statistics failed to fetch the value of backup MAC address correctly. [PR1577611](#)
- Native sensors does not work for LDP LSP, LDP p2mp sensor. [PR1577931](#)
- The bbe-smgd process crash might be seen when the RADIUS server sends multiple CoA. [PR1578162](#)
- Mismatch in the snapshot recovery steps display message. [PR1578556](#)
- TACACS traffic might be dropped. [PR1578579](#)
- High FPC CPU usage might be seen when signal on the link is unstable. [PR1579173](#)

- Random or silent reboot might be seen. [PR1579576](#)
- On the MPC11E line card, system resource monitor does not list some of the available Packet Forwarding Engines. [PR1579975](#)
- On MX Virtual Chassis, data is missing in gRPC based components or sensor output. [PR1580120](#)
- Authentication might fail if the password contains special characters. [PR1580003](#)
- When analyzers mapped to channelized port, then the mirror might not happen properly. [PR1580473](#)
- BFD session with in-line mode might flap during network congestion. [PR1580320](#)
- The l2cpd process might crash on dual Routing Engines. [PR1580479](#)
- More than one subscriber on same VLAN fails to apply same FWF template. [PR1580826](#)
- Need to add support for Virtual Chassis licensing. [PR1580880](#)
- Issue is observed in telemetry when the set services analytics streaming-server configuration is present and server is not reachable. [PR1581192](#)
- Memory leak might happen due to stale NAT64 entries. [PR1581231](#)
- VM core messages are generated at 0xffffffff80443eef in kern_reboot. [PR1581260](#)
- The rpd process might crash on the new primary after performing graceful switchover. [PR1581878](#)
- Changing bandwidth statement does not take affect for SNMP ifHigSpeed oid until a PSX interface is disable/enabled. [PR1582060](#)
- The l2ald process generates the core file in l2ald_vxlan_if1_create_event_handler while running the EVPN VXLAN scripts in VQFX during the PCT submission. [PR1582128](#)
- Communication between two CE devices might be failed when BGP rib-sharding is enabled. [PR1582210](#)
- Pciephy and firmware download are not working after migration to 6.5.19. [PR1582244](#)
- The bbe-smgd process on both routing engines might crash due to a rare timing issue after log out of subscribers over pseudowire. [PR1582356](#)
- On MX960 devices, the 400G and 4x100G optics laser restores after reboot despite interface disable being configured. [PR1582418](#)
- Destination port might be incorrectly set on MS-MPC and MS-MIC in a DS-Lite scenario. [PR1582595](#)

- Node locked license addition fails. [PR1582704](#)
- Configuring or removing the hierarchical-scheduler or per-unit-scheduler might cause traffic to stop forwarding. [PR1582724](#)
- The firewall filter logs are incorrectly populated the protocol entries. [PR1582780](#)
- Reset JBS, JAS, JPS definition to align with Hawk License model. [PR1583438](#)
- Reset PFL, AFL definition to align with Hawk License model. [PR1583439](#)
- SNMP SysObjectID.0 is empty with enabled unified-services. [PR1583534](#)
- TCP connection to syslog server might fail to be established after adding tcp-log configuration for an existing service set. [PR1583979](#)
- The jsd process hogging CPU. [PR1584357](#)
- Traffic might not get filtered properly when security-intelligence profile is configured on the MX platforms. [PR1584377](#)
- The rpd process might crash due to a rare timing issue if both BGP Local-RIB and Adjacency-RIB-In route monitoring are enabled in BMP. [PR1584560](#)
- Bridge domain names information is not displayed properly in the show bridge statistics instance command. [PR1584874](#)
- After changing configuration, the show bridge statistics command displays extreme larger value. [PR1584876](#)
- Traffic impact might be seen when tunnel-services bandwidth is configured. [PR1584969](#)
- GRE OAM packets are sent through queue 0 with force-control-packets-on-transit-path statement enabled. [PR1586169](#)
- Traffic drop after enabling flexible-queuing-mode on MPC2E line cards. [PR1586403](#)
- The l2ald process might crash on changing the routing-instance. [PR1586516](#)
- Inter and intra VNI traffic drop might occur in spine with EVPN-VXLAN CRB configuration. [PR1586537](#)
- The rpd process generates core file if the show igmp continuous stats command is executed after GRES. [PR1587023](#)
- Mspmand.core.ms32.0.gz is found while testing memory-usage prints garbage value. [PR1587103](#)
- The SNMP trap for MAC notifications might not be generated when an interface is added explicitly under switch-options. [PR1587610](#)

- The bbe-smgd might crash if the staled ACI based subscribers are not cleaned up properly. [PR1587792](#)
- The na-grpc process crash might be seen and existing telemetry connections will be disconnected. [PR1587956](#)
- The rpd process crash might be observed on the router running in a scaled setup. [PR1588439](#)
- The bbe-statsd memory leak might be observed on backup Routing Engine during subscriber's login and logout. [PR1589081](#)
- The jsd process crash might be seen in a rare condition in a telemetry scenario. [PR1589103](#)
- The l2cpd process might crash. [PR1589216](#)
- Allow default license for FBF, CFM, VRRP, Q-IN-Q, MC_LAG, TIMING, IGMP, PIM, GRE_TUNNEL, RIP, OSPF, Virtual Chassis, and sFlow. [PR1589920](#)
- Expected snooping route is not observed after configuring one bridge with snooping and add interface check. [PR1590278](#)
- Some times show chassis fabric reachability extended detail command shows that fabric healing is complete for Phase 2, while the links to few FPCs or SLCs are still under training. [PR1590335](#)
- Traffic loss might be observed due to FPC crash in a scaled subscriber scenario. [PR1590374](#)
- If the CoS CR-features used by VBF service is configured, MPC might crash with subscriber [PR1591533](#)
- The clear-ipsec-sas-for-duplicate-ts is not clearing secur Access (SA) for duplicate traffic selectors (TS). [PR1591735](#)
- The xSTP might not get configured when it is enabled on a interface with SP style configuration on all platforms. [PR1592264](#)
- Routing Engine kernel might crash due to logical interfaces of aggregated interface adding failure in Junos OS kernel. [PR1592456](#)
- Any mmcq based services might crash due to shared memory queue issue happens in a rare condition. [PR1592889](#)
- The TCP keepalive message might not be processed by the private network host. [PR1593226](#)
- Fabric errors will be generated after swapping MPC10E with MPC7E line card in the same slot. [PR1593821](#)
- On MX5, MX40, and MX80 routers, TEB stuck in present state. [PR1595107](#)

- On MX Series platforms with EVPN-VXLAN with shared-tunnel configuration, when there is BGP flap or restart of I2ald, then info logs appear. [PR1595203](#)
- The I2ald process might crash on all leaves and spines after a new leaf is added to the EVPN fabric. [PR1596229](#)
- Traffic loss might happen periodically in MACsec used setup if Routing Engine is working under a pressure situation. [PR1596755](#)
- Major alarms on all FPCs in chassis after some time from boot up. [PR1597066](#)

Class of Service (CoS)

- The explicit classifier or rewrite-rule might not work as expected for a logical interface if the wildcard configuration is also applied. [PR1556103](#)
- On the MPC7E line card, the BPS counter of the egress queue displays incorrect BPS value when the cell mode is configured on the static interface. [PR1568192](#)
- FPC crash might be observed after the show class-of-service command execution. [PR1568661](#)
- Class of service commands will be auto sorted and will not be ordered as per the user configuration. [PR1568907](#)
- Unable to configure policer with bandwidth-limit greater than 50g. [PR1575049](#)

EVPN

- Rpd memory leak might occur when the EVPN configuration is changed. [PR1540788](#)
- The rpd process might crash after adding route-target on a dual Routing Engine system under the EVPN multihoming scenario. [PR1546992](#)
- The rpd process might crash under EVPN-VPWS environment. [PR1562160](#)
- Prefix added to the mhevpn.evpn.0 output route table triggers TC failure. [PR1566429](#)
- Traffic might drop on multicast based VXLAN tunnel. [PR1567209](#)
- Policy with mac-filter-list might not work if the change is not related to that policy committed in an EVPN scenario. [PR1567623](#)
- ESI preference is not preferred when configured on lo0 for multicast VXLAN. [PR1570618](#)
- The multicast traffic loss might be seen in EVPN VXLAN scenario with CRB multicast snooping [PR1570883](#)

- The mustd process generates core file during upgrading or while committing a configuration. [PR1577548](#)
- Rpd process might crash in high scaled EVPN VXLAN scenario. [PR1581674](#)
- Multicast traffic loss might be seen in EVPN setup with IGMP snooping used. [PR1582134](#)
- After the 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](#)
- The BUM traffic might lose after triggering GRES+NSR in an EVPN-MPLS or EVPN-ETREE scenario. [PR1586402](#)
- The traffic might be dropped when EVPN and L3VPN routes are resolved using the same MPLS-over-UDP tunnel. [PR1587204](#)
- The traffic might be dropped in an EVPN-VXLAN multihomed scenario. [PR1590128](#)

Forwarding and Sampling

- After routing restarts, the remote mask that the routing daemon sends might be different from the existing remote mask that the Layer 2 learning daemon had before restart. [PR1452990](#)
- User-defined ARP policer is not applied on aggregated Ethernet interface until firewall process is restarted. [PR1528403](#)
- The dfwd process might crash when implementing non-contiguous firewall filter. [PR1555724](#)
- The configuration archive transfer-on-commit fails. [PR1563641](#)
- In the VXLAN scenario, the locally originated packets have UDP source port 0. [PR1571970](#)
- The pfded memory leak might be observed. [PR1573285](#)
- The l2ald process might crash on changing the routing-instance. [PR1584737](#)

General Routing

- The ndp process might reach to 100 percent and might result in traffic drop. [PR1551644](#)
- More memory usage might occur in ndpd (NDP daemon). [PR1568370](#)
- Silent switchover might be triggered on executing restart routing. [PR1570993](#)
- The DHCP ALQ is not working as expected. [PR1578543](#)
- Rpd process core file might be seen on the backup Routing Engine after a switchover with graceful restart is enabled. [PR1582095](#)

- After performing NSSU, timeout waiting for response from fpc0 error message is seen while checking version detail. [PR1584457](#)

Infrastructure

- On Virtual Chassis and Virtual Chassis fabric, HEAP malloc(0) detected. [PR1546036](#)
- When device trying reboot from OAM might get stuck in OK prompt and leading to reboot from Junos OS. [PR1555748](#)
- Some MAC addresses might not be aged out. [PR1579293](#)

Interfaces and Chassis

- Backup Routing Engine or backup node might get stuck in bad status with improper backup-router configuration. [PR1530935](#)
- On the MPC10 line card, DMRs or SLRs are not received with an EVPN up MEP on the aggregated Ethernet interface with normalization. [PR1543641](#)
- An lacpd core file is observed after router reboot. [PR1553196](#)
- Block duplicate IP across different logical interfaces inside same routing instance. [PR1555861](#)
- Sessions are flapped after applying the action profile on the router. [PR1561044](#)
- The input errors counter command on the monitor interface command does not work. [PR1561065](#)
- The ppmd process might crash when VRRP is configured. [PR1561281](#)
- MAC address entry issue might be observed after the MC-LAG interface failover. [PR1562535](#)
- Traffic loss might be seen while verifying VRRP state machine functionality. [PR1564551](#)
- Unable to set member-id as Routing Engine is in synching mode forever when its having invalid Virtual Chassis data. [PR1569556](#)
- The show interface interface name | display xml command output displays the media type if-media-type also along with other parameters. [PR1574035](#)
- There might be increase in memory for the fabspoked process. [PR1574391](#)
- MX Virtual Chassis ISSU incompatible FRU offline can result in unexpected FPC restarts after ISSU completes. [PR1575687](#)

- The following errors are generated during GRES: VRRPMAN_PATRICIA_GROUP_ADD_FAIL: vrrp_ifcm_send_bulk: Failed to add group to patricia tree key and VRRPMAN_ENTRY_KEY_PRESENT: vrrp_ifcm_send_bulk: Already an entry present with the key. [PR1575689](#)
- MC-AE interfaces might go down if same VRRP group-id is configured on multiple IRB units. [PR1575779](#)
- The show interface description display order is different. [PR1576224](#)
- Newly added MC-LAGs do not come up after Routing Engine switchover. [PR1583547](#)
- NCP/PPP negotiation Max-Failure retry count are not configurable. [PR1584168](#)
- Unable to configure pseudowire interface on an MX10003 in Virtual Chassis mode. [PR1587499](#)
- The VRRP host cannot be reached if native-vlan-id is configured. [PR1595896](#)

Intrusion Detection and Prevention (IDP)

- Adding signature in packet drop reason and sending to record packet drops module. [PR1574603](#)

J-Web

- J-Web allows a locally authenticated attacker to escalate their privileges to root. [PR1511853](#)
- To improve performance in Monitoring > Network > Interfaces page, Admin Status is removed, Services and Protocols data merged into one Host inbound traffic. [PR1574895](#)

Juniper Extension Toolkit (JET)

- TCP connection might not be established while creating the default gRPC channel with fw_channel name. [PR1559064](#)
- The custom JET APP will be lost after rebooting. [PR1570563](#)

Junos XML API and Scripting

- Multiple vulnerabilities in cURL resolved. [PR1562153](#)

Layer 2 Features

- LACP gets into detached state when deleting VLAN on aggregate interface configured on SP style. [PR1555862](#)

- Traffic forwarding for VLAN 2 might not be correct when a VLAN member is removed from the ESI interface. [PR1570446](#)
- LACP does not come up in non-oversubscribed mode for a set of ports. [PR1563171](#)
- The `clear vpls mac-address` could result in rpd core. [PR1573406](#)

Layer 2 Ethernet Services

- The copying of files to the RCB over WAN ports is slow. [PR1496895](#)
- Aggregated Ethernet interface flap might be seen during NSSU. [PR1551925](#)
- DHCP packet drop might be seen when the DHCP relay is configured on a leaf device. [PR1554992](#)
- In a DHCP relay configuration with active lease query, some subscriber's active on master might get logged out. [PR1559269](#)
- Receipt of malformed DHCPv6 packets causes jdhcpd process to crash and restart. [PR1564434](#)
- DHCPv6 option 18 and option 37 might not be created in a DHCP dual stack scenario. [PR1564778](#)
- The `jnxJdhcpLocalServerMacAddress (.1.3.6.1.4.1.2636.3.61.61.1.4.3)` returns incorrect format of the MAC address. [PR1565540](#)
- The Option 82 information is incorrectly cleared by the DHCP relay agent. [PR1568344](#)
- The DHCP client will be offline for 120 seconds after sending the DHCPINFORM message in a the DHCP relay scenario. [PR1575740](#)
- DHCP relay drops packets during the renewal DHCP process. [PR1576417](#)
- The jdhcpd might crash if the relay-source lo0 is enabled in the DHCP relay. [PR1580724](#)
- The jdhcpd process might not respond to any discover message when it is in clients waiting to be restored state. [PR1592552](#)

MPLS

- The rpd process might crash in a corouted bidirectional RSVP LSP scenario. [PR1544890](#)
- A new LSP might not be up even if bypass LSP is up and setup-protection is configured. [PR1555774](#)
- Incorrect EXP bit change might be seen in certain conditions under MPLS scenario. [PR1555797](#)
- MPLS-LIB memory leak might be seen in segment routing scenario. [PR1556495](#)

- Traffic loss might be observed during rpd crash when RSVP signaled P2MP LSP is configured. [PR1559022](#)
- LDP routes might be stuck when BGP LU session is down. [PR1562884](#)
- Traffic sent over an LSP might be dropped if two consecutive PLRs along the LSP perform local repair and bypass protecting the second PLR fails. [PR1566101](#)
- Unexpected LSP packet count is found in the ingress MPLS LSP statistics. [PR1570382](#)
- The rpd process generates core file when deactivating PCEP protocol followed by RSVP protocol. [PR1579370](#)
- The suboptimal routing issues might be seen in case LDP route with multiple next hops. [PR1582037](#)
- Add lsp-ping-multiplier option support for LDP-OAM similar to RSVP-OAM. [PR1582254](#)
- MBB is not triggered when LSP is reverting back to primary path. [PR1587704](#)

Multicast

- FPC might crash in a multicast scenario. [PR1569957](#)

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

- The mib2d process crashes and generates a core file on backup Routing Engine. [PR1557384](#)
- Context registration from l2cpd to snmpd might fail after l2cpd service restart. [PR1561736](#)
- SSH connection might become unresponsive and logs the following message: kern.maxfiles limit exceeded by uid. [PR1567634](#)
- Slow memory leak might be observed for snmpd process. [PR1575790](#)

Platform and Infrastructure

- Traffic loss might be observed due to FPC crash on MX platforms. [PR1482683](#)
- Interwork failure as RPM client and TVP platforms as RPM server (and vice versa). [PR1508127](#)
- Console access on backup Virtual Chassis member is not allowed. [PR1530106](#)

- The npc process generates the core file in `igmp_process_wakeup_events,igmp_pfe_thread,thread_detach_tty`. [PR1534542](#)
- Packets transiting via multicast-based VXLAN VTEP interface might be dropped post FPC restart. [PR1536364](#)
- The `queue-counters-srx-reserved-buffer-bytes` count is 625000 bytes, expected buffer is 2500000. [PR1538286](#)
- The following major error message might cause the Packet Forwarding Engine to disable:
`XQ_CMERROR_SCHED_L3_PERR_ERR`. [PR1538960](#)
- Subscribers over an interface-set might not be able to login. [PR1539260](#)
- The kernel might crash if GRES is performed on either new iteration or after swapping the Routing Engine and restoring the HA configuration. [PR1549656](#)
- Traffic loss might be seen as logical interface policer is not processed properly during filter migration. [PR1551394](#)
- Traffic is not forwarded over IRB to a Layer 2 circuit on the It interfaces. [PR1554908](#)
- SPC3 might not come up after the system reboot. [PR1555904](#)
- The IPv4 EXP rewrite might not work properly when `inet6-vpn` is enabled. [PR1559018](#)
- The BUM frame might be duplicated on an aggregate device if the extended-port on the satellite device is an aggregated Ethernet interface. [PR1560788](#)
- Interfaces statistics not updated on aggregated Ethernet interface as expected with CCOAE configurations. [PR1561304](#)
- Multicast traffic with incorrect source MAC address might be observed from IRB interface. [PR1561313](#)
- The DHCPv4 request packets might be incorrectly dropped when DDoS attack occurs. [PR1562474](#)
- Traffic loss might be observed due to FPC crash on MX platforms. [PR1563144](#)
- The mtr process might hog CPU when the traceroute monitor command is paused. [PR1563298](#)
- The `enforce-strict-scale-limit-license` configuration enforces subscriber license incorrectly in the ESSM subscriber scenario. [PR1563975](#)
- The Last `flapped` timestamp for interface `fxp0` gets reset every time the `monitor traffic interface fxp0` command is executed. [PR1564323](#)
- PFEX might crash when soft error recovery feature is enabled on Packet Forwarding Engine. [PR1567515](#)

- Reclassify the severity of the CMERROR XMCHIP_CMERROR_DDRIF_PROTECT_WR_RD_SRAM_RUNN_CHKSM from major to minor. [PR1568072](#)
- The following error message is observed: toe_lu_stats_ucode core found @ jbeta_fcv_alloc_fcv_idx_global jbeta_sfilter_fcv_cb bwy_dfw_sfilter_fcv_cb. [PR1569328](#)
- The following error message is observed: pfe_err-jnh_physmem_add_resvd_to_cntr(18014): PFE 0 jnh_app 0x08020860, add 0x00080000 from 0x00b00000-0x00b80000 to baMask 0x1. [PR1570631](#)
- FPCs might crash randomly while deleting the interface-set in the system. [PR1571192](#)
- When EVPN-VXLAN is 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 exhausted the FPC might reboot. [PR1571439](#)
- Scale-subscriber license might not be updated properly on the backup Routing Engine which leads to License grace period for feature scale-subscriber(44) is about to expire alarm after GRES. [PR1573289](#)
- The following error message is observed: cassxr_err_addr(8593): Uninitialized Read Error @ EDMEM[0x7cb601b0]. [PR1573920](#)
- Introduce two new major CMERRORs for XM chip-based line card to stabilize the running device. [PR1574631](#)
- Memory partitioning issue might happen on Packet Forwarding Engine after applying sampling and the flex-flow-sizing to the MX Series with MPCs/MICs based line-cards. [PR1575994](#)
- If committing the source-address addr routing-instance and then delete the source-address addr in private edit mode, commit fails with a warning message. [PR1582529](#)
- VRRP device originally taking backup role might cause destination IP unreachable after VRRP mastership switch-over. [PR1584115](#)
- FPC crash might be observed in a scaled firewall configuration on MX Series platforms. [PR1586817](#)
- The traffic might not failover with shared-bandwidth-policer enabled on aggregated Ethernet. [PR1588708](#)

Routing Policy and Firewall Filters

- Global variable policy_db_type is not set to the correct value on failure. [PR1561931](#)
- Generated route goes to the hidden state when the protect core command is enabled. [PR1562867](#)
- The rpd process might crash when the deletion of routing table occurs. [PR1565629](#)

- The rpd might crash due to the source-address-filter-list enabled within the policy. [PR1565891](#)
- Traffic loss might be observed during rpd process crash when auto-bandwidth is configured. [PR1579830](#)
- The bbe-smgd process fails when reading configuration for address mask prefix-length when configured in a policy statement, causing the service profile to fail. [PR1583535](#)

Routing Protocols

- The rpd process crashes when a fresh router is configured with IS-IS and RIB-group to leak inet3 routes from no-forwarding to primary instance in single commit. [PR1534486](#)
- Unexpected packet loss might happen due to inet-vpn routes not valid in vrf.inet.0 and bgp.l3vpn.0 routing tables. [PR1543717](#)
- Convergence time is high when the IGMP snooping configuration is deleted. [PR1550523](#)
- Specific packets can trigger rpd crash when BGP origin validation is configured with RPKI. [PR1556207](#)
- Route validation states might flip between VALID, INVALID, and UNKNOWN in some corner case. [PR1556656](#)
- Multipath information is displayed for BGP route even after disabling the interface for one path. [PR1557604](#)
- BGP-LU session flap might be seen when the AIGP is used. [PR1558102](#)
- The ISO routes are not leaked in default (master) instance after switchover or reconfiguration. [PR1558532](#)
- Traffic loss might occur for stitched traffic from segment routing towards LDP if no-eligible-backup is configured. [PR1558565](#)
- When admin-color based policy evaluation happens with the policy LFA configuration, the backup next hop chosen (among the possible different backup next hops) might not be correct. [PR1558581](#)
- Incorrect Active, Received, or Accepted counters in the show bgp summary command. [PR1558678](#)
- The rpd process might crash when applying the BGP route policy change. [PR1560037](#)
- VPN routes learned from core were not advertised to the CE devices when BGP sharding is configured. [PR1560661](#)
- All the Layer 3 VPN route resets when a VRF is added or removed. [PR1560827](#)
- Duplicate LSP next hop is shown on inet.0, inet.3 and mpls.0 route table when ospf traffic-engineering shortcuts and mpls bgp-igp-both-ribs are enabled. [PR1561207](#)

- Incorrect SPF calculation might be observed for OSPF with `ldp-synchronization hold-time` configured after the interface flap. [PR1561414](#)
- The `ppmd` memory leak might cause traffic loss. [PR1561850](#)
- The `rpdd` process might crash with dynamic tunnels configured. [PR1562458](#)
- The `rpdd` process might crash on the backup Routing Engine after `rpdd` process restart is triggered on the primary Routing Engine. [PR1563350](#)
- The `rpdd` process might crash if there are more routes changed during the `commit-sync` processing window. [PR1565814](#)
- There might be traffic loss when GRE interface flaps. [PR1566428](#)
- The `rpdd` process might crash in BGP L2VPN scenario due to memory corruption. [PR1567026](#)
- The `rpdd` process might crash when the BGP session re-establishes or flaps. [PR1567182](#)
- The `rpdd` memory leak might be observed during CLI or ephemeral commits in a OSPFv2 scenario. [PR1568157](#)
- Traffic loss might be observed due to the `rpdd` process crash in BGP multipath scenario. [PR1568600](#)
- The `rpdd` process might crash continuously when MoFRR is configured along with TI-LFA. [PR1568750](#)
- Traffic might be lost during mirror data transmit from the primary `ppmd` or `bfdd`. [PR1570228](#)
- There might be 10 seconds delay to upload the LSP on the point-to-point interface if `rpdd` process is restarted on its direct neighbor. [PR1571395](#)
- SNMP MIB `ospfv3NbrState` is returning drifted value. [PR1571473](#)
- Incorrect authentication-algorithm is set in BGP neighbor. [PR1571705](#)
- `Rpdagent` core seen while testing BFD state replication. [PR1571824](#)
- After first parallel ISSU, subsequent ISSU aborts with `Aborting Daemon Prepare` due to BFD abort state. [PR1572265](#)
- The DHCP BFD subscriber session does not come up on the MPC Type 2 card and gets stuck in the `Down` state. [PR1572577](#)
- The DHCP packets might be dropped in the Static VXLAN scenario. [PR1576168](#)
- Provide a CLI option to change default BGP listen port. [PR1576728](#)
- The `ppmd` might crash when enabling MD5 authentication on OSPF with BFD flapping. [PR1576893](#)

- BGP session flap might be observed after the Routing Engine switchovers when the VRRP virtual address is used as the local address for the BGP session. [PR1576959](#)
- Multicast traffic loss might be observed due to logical PIM de-encapsulation interface is not created as expected. [PR1577461](#)
- The rpd process might crash when two or more routing instances are deleted in one shot. [PR1578740](#)
- The dcufe process might crash when any interface flaps. [PR1579736](#)
- Rpd core found at thread_next_node jnx_bgp_tunnel_encaps_attr_tunnel_count jnx_bgp_tunnel_encaps_attr_set_tunnel. [PR1579818](#)
- BGP replication might be stuck in rare and timing conditions. [PR1581578](#)
- BGP session carrying VPNv4 prefix with IPv6 next hop might be dropped. [PR1580578](#)
- The rpd process might crash in BGP and MPLS scenarios. [PR1581794](#)
- The route resolution issue is observed after controller facing Packet Forwarding Engine restart or core interface disable or enable [PR1581845](#)
- Possible rpd process might crash with the routing-options transport-class configuration during the restart. [PR1582081](#)
- The voice VLAN might not get assigned to the access interface. [PR1582115](#)
- With IGMP snooping implemented, there is unexpected jitter issue that could cause traffic loss. [PR1583207](#)
- SSH cipher option Triple-DES is disabled in FIPS mode. [PR1583470](#)
- The rpd process crash might be seen in certain IS-IS scenario. [PR1583484](#)
- On rare occasion, rpd process core might be observed on backup Routing Engine after loading a new image. [PR1583630](#)
- Origin-validation replication status shows up in the show task replication command output even when it is not configured. [PR1583692](#)
- The rpd process might crash when BGP RPKI session record-lifetime is configured less than the hold-time. [PR1585321](#)
- The rpd process might crash after committing with the configured static group. [PR1586631](#)
- Incorrect BGP next-hop advertisement in a L3VPN scenario. [PR1587879](#)
- The multicast traffic loss might be observed after unified ISSU is performed. [PR1588555](#)

- The rpd process might crash in a scaled routing instances scenario. [PR1590638](#)
- when you disable or enable BGP in a short time interval on a scaled NSR router can result in backup rpd process restart. [PR1591717](#)
- The remote LFA backup path might not be formed. [PR1592424](#)
- BGP egress-TE routes lose to BGP routes using the same protocol preference. [PR1593332](#)
- The routing process might crash due to memory corruption while processing BGP multipath route. [PR1594626](#)

Services Applications

- The CoA with LI-on or LI-off message might be dropped during CoA process. [PR1554618](#)
- Memory leak might be observed in a tunnel flapping scenario. [PR1567291](#)
- Support to clear l2tp session based on routing-instance name filter. [PR1580984](#)
- IWF AVP value might not be reflected properly on LTS. [PR1581096](#)

Subscriber Access Management

- BBE-SMGD configures incorrect vbf_accurate_accounting_bits to the Packet Forwarding Engine. [PR1515899](#)
- The authd might crash after performing unified ISSU in a MX BNG scenario. [PR1570096](#)
- CoA request might not be processed correctly from time to time. [PR1571501](#)

User Interface and Configuration

- The port_speed configuration details not present in the picd configuration for ports et-0/0/128 and et-0/0/129. [PR1510486](#)
- The configuration under groups stanza is not inherited properly. [PR1529989](#)
- Commit might fail after the Routing Engine switchovers. [PR1531415](#)
- The operational state would be incorrect on the system and CoS schedulers configuration change might not take effect. [PR1536615](#)
- The mgd process might crash when performing rollback command. [PR1554696](#)
- The chassisd core files might be observed if PIC number 2 or 3 is used on MX204 platforms. [PR1555685](#)

- If the xml output from the request `vmhost mode test | display xml rpc` command is picked and used in NETCONF fails. [PR1559786](#)
- Memory leak on eventd might be seen when running the request system script `event-scripts reload` command. [PR1570580](#)
- The LACP might stop working after disabling LACP sync-reset. [PR1576146](#)

Virtual Chassis

- Virtual Chassis might not come up after upgrade when QSFP+-40G-SR4, QSFP+-40G-LR4, or QSFP+40GE-LX4 is used. [PR1579430](#)

VPNs

- Traffic from the reverse direction might cause traffic loss for up to 1 second with NSR switchover. [PR1558395](#)
- Type7 messages might not be sent from egress PE device resulting in Type 3 or Type 5 messages not created for some S, Gs in source PE devices. [PR1567584](#)
- The rpd might crash during a race condition under BGP multipath scenario. [PR1567918](#)
- The iked process might crash when IKEv2 negotiation fails on MX devices. [PR1577484](#)
- The rpd process might crash in the NG-MVPN scenario. [PR1579963](#)
- The traffic of the draft-rosen multicast VPN might lose after switching over the Routing Engines. [PR1584720](#)

Documentation Updates

There are no errata or changes in Junos OS Release 21.2R3 documentation for the MX Series routers.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading to Release 21.2R3 | 223](#)
- [Procedure to Upgrade to FreeBSD 12.x-Based Junos OS | 223](#)
- [Procedure to Upgrade to FreeBSD 6.x-Based Junos OS | 226](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 228](#)
- [Upgrading a Router with Redundant Routing Engines | 228](#)
- [Downgrading from Release 21.2R3 | 229](#)

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 21.2R3, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS 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 21.2R3

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

- For 64-bit Routing Engine version:

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

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

- For 32-bit Routing Engine version:

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

- For 64-bit Routing Engine version:

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

Replace source with one of the following values:

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

- `ftp:// hostname/ pathname`
- `http:// hostname/ pathname`
- `scp:// hostname/ pathname`

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 21.2R3, 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 21.2R3 `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](#).

Procedure to Upgrade to FreeBSD 6.x-Based Junos OS

Products impacted: MX5, MX10, MX40, MX80, MX104.

To download and install FreeBSD 6.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:

```
user@host> request system software add validate reboot source/jinstall-ppc-20.4R1.9-
signed.tgz
```

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

```
user@host> request system software add validate reboot source/jinstall-ppc-20.4R1.9-
limited-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*

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.

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: After you install a Junos OS Release 21.2R3 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.

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 21.2R3

To downgrade from Release 21.2R3 to another supported release, follow the procedure for upgrading, but replace the 21.2R3 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 | 230](#)
- [What's Changed | 232](#)
- [Known Limitations | 233](#)
- [Open Issues | 233](#)
- [Resolved Issues | 235](#)
- [Documentation Updates | 237](#)
- [Migration, Upgrade, and Downgrade Instructions | 238](#)

These release notes accompany Junos OS Release 21.2R3 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 21.2R3 | 230](#)
- [What's New in 21.2R2 | 230](#)
- [What's New in 21.2R1 | 230](#)

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

What's New in 21.2R3

There are no new features or enhancements to existing features for NFX Series devices in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for NFX Series devices in Junos OS Release 21.2R2.

What's New in 21.2R1

IN THIS SECTION

- [Application Identification \(AppID\) | 230](#)
- [Authentication and Access Control | 232](#)
- [Flow-Based and Packet-Based Processing | 232](#)

Learn about new features or enhancements to existing features in this release for the NFX Series.

Application Identification (AppID)

- **Application-based multipath routing (AMR) improvements (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, SRX550 HM, and vSRX)**—Starting in Junos OS release 21.2R1, we've introduced the following improvements for AMR:

- Support for the traffic in reverse direction
- Queuing mechanism for out-of-order packets at the receiving device
- Association of AMR rules and service-level agreement (SLA) rules with advanced policy-based routing (APBR) rule in an APBR profile
- Link selection option that includes overlay interfaces such as GRE and secure tunnel
- Enablement of AMR in one of the two modes—SLA violation mode or standalone mode
- Support for IPv6 traffic
- Support for AMR over IPsec and GRE sessions

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

- **Multicast support in SD-WAN deployments (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX4100, SRX4200, SRX4600, vSRX)**—Starting in Junos OS Release 21.2R1, we've added support for multicast traffic on SRX Series devices in Provider Edge (PE) for SD-WAN deployments. The support for multicast traffic is available when the security device is operating with forwarding option set as flow-based.

Support for multicast traffic results in bandwidth preservation and more efficient traffic flows.

See [[mode \(Security Forwarding Options\)](#) and [Virtual Routing and Forwarding Instances in SD-WAN Deployments](#)].

- **SLA link preference enhancement (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, SLA link preference for security device interfaces supports custom link tags. You can define the link preferences using the preferred-tag and affinity options.

This enhancement allows application traffic to switch from a lower-priority link to a higher-priority link that meets SLA requirements.

[See [Understanding Link-Type Affinity for the Preferred Link](#) and [sla-rule](#).]

- **Application-based load balancing support for APBR (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, security devices support application-based load balancing for advanced policy-based routing (APBR). The APBR achieves load balancing by moving the application traffic in multiple WAN links using user-defined link selection criteria. The link selection criteria for application traffic depends on the link tag and link priority preference settings you defined for the advanced policy-based routing (APBR) interface. The application traffic distribution through the selected links depends on the link weight configuration.

This feature improves the application traffic distribution performance for APBR and application quality of experience (AppQoE).

[See [Advanced Policy-Based Routing](#), [sla-options](#), and [interface](#).]

Authentication and Access Control

- **Display dynamic-applications and URL category hit counts in a security policy (NFX Series and SRX Series)**—Starting in Junos OS Release 21.2R1, we've enhanced the `show security policies hit-count` command to include the dynamic applications and URL categories options. You can now display the utility rate of the policy according to the number of hits for the dynamic applications and URL categories.

[See [show security policies hit-count](#).]

Flow-Based and Packet-Based Processing

- **GRE acceleration enhancement (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.2R1, security devices support the existing PMI and GRE acceleration for non software-defined WAN (SD-WAN) deployments.

PMI and GRE acceleration improve GRE and MPLS-over-GRE performance.

[See [gre-performance-acceleration](#) and [show security flow status](#).]

- **Multicast support in SD-WAN deployments (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, we've added support for multicast traffic on security devices in Provider Edge (PE) for SD-WAN deployments. The support for multicast traffic is available when the security device is operating with forwarding option set as flow-based.

Support for multicast traffic results in bandwidth preservation and more efficient traffic flows.

[See [mode \(Security Forwarding Options\)](#) and [Virtual Routing and Forwarding Instances in SD-WAN Deployments](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 233](#)
- [What's Changed in Release 21.2R2 | 233](#)

- [What's Changed in Release 21.2R1 | 233](#)

Learn about what changed in Junos OS main and maintenance releases for NFX Series devices.

What's Changed in Release 21.2R3

There are no changes in behavior and syntax in Junos OS Releases 21.2R3 for NFX Series devices.

What's Changed in Release 21.2R2

There are no changes in the behavior of Junos OS features or in the syntax of Junos OS statements and commands in Junos OS Release 21.2R2 for NFX Series devices.

What's Changed in Release 21.2R1

There are no changes in the behavior of Junos OS features or in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for NFX Series devices.

Known Limitations

There are no known limitations in hardware or software in Junos OS Release 21.2R3 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 | 234](#)
- [High Availability | 234](#)
- [Interfaces | 234](#)
- [Platform and Infrastructure | 234](#)

Learn about open issues Junos OS Release 21.2R3 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](#)

High Availability

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

Interfaces

- (Applies to an NFX350 device with MACsec on the layer 2 interfaces) After you reboot an NFX350 device or restart the Packet Forwarding Engines on the device, the MACsec connectivity is not established on some of the links.
As a workaround, delete the layer 2 interface configuration for the affected links and then reconfigure it. [PR1640451](#)

Platform and Infrastructure

- During FTP on NFX150 devices, the following error message appears:

```
tpd[14105]: bl_init: connect failed for `/var/run/blacklistd.sock' (No such file or directory)
```

[PR1315605](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.2R3 | 235](#)
- [Resolved Issues: 21.2R2 | 235](#)
- [Resolved Issues: 21.2R1 | 236](#)

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R3

IN THIS SECTION

- [Interfaces | 235](#)

Interfaces

- 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: 21.2R2

IN THIS SECTION

- [Interfaces | 236](#)
- [Intrusion Detection and Prevention \(IDP\) | 236](#)
- [Performance Modes | 236](#)
- [Platform and Infrastructure | 236](#)

Interfaces

- Unable to configure destination-port on firewall filter on NFX250 NextGen devices. [PR1592019](#)
- On NFX Series devices, deletion of a VNF interface that is mapped to a SR-IOV interface fails. [PR1598993](#)
- L3 data plane interfaces are not appearing when flex mode is enabled on NFX350-S3 devices. [PR1599643](#)

Intrusion Detection and Prevention (IDP)

- IDP predefined-attack-groups "Enterprise - Recommended" policy load fails on NFX250 NextGen devices due to insufficient heap memory on the data plane. [PR1588881](#)

Performance Modes

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

Platform and Infrastructure

- When the available free physical memory drops below 1.5 GB, configuration commits by Junos Device Management Daemon (JDMD) might not take effect and mustd core files are seen. This issue does not have any impact on the running traffic. [PR1599641](#)

Resolved Issues: 21.2R1

IN THIS SECTION

- [Interfaces | 236](#)
- [Performance Modes | 237](#)
- [Platform and Infrastructure | 237](#)

Interfaces

- On NFX250 devices, a VNF interface is not brought down when the VNF interface is mapped to an already link down or disabled peer physical interface. [PR1555193](#)

Performance Modes

- You cannot enable the trust mode on an SR-IOV virtual function assigned to a VNF. [PR1593037](#)
- A message is provided in syslog if reboot is required for the mode modification to take effect in custom mode. [PR1555465](#)

Platform and Infrastructure

- 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](#)
- On NFX350 devices and the SRX5000 line of devices with SPC3 card, the DPD Gateway failover feature is not supported. [PR1564715](#)
- The l2cpd core files might be seen on reboot. [PR1561235](#)
- On NFX150 devices, when J-Flow v5 is configured and the J-Flow v5 server is reachable through an IPsec tunnel, and the MTU size of this IPsec tunnel is configured as 1500, the J-Flow packets are not generated on NFX Series devices. As a workaround, use J-Flow v9 or IPFIX version, instead of J-Flow v5, to enable the J-Flow functionality on NFX Series devices. [PR1539964](#)
- You can transfer file from USB to hypervisor by enabling the usb-pass-through functionality. [PR1535220](#)
- On NFX150, NFX250 NextGen, and NFX350 devices, the `EmulatorPin CPUSet` option does not get configured, which might result in vCPU running on a higher level up to 100%. [PR1540564](#)
- The DSL SFP firmware cannot finish upgrade successfully through vmhost reboot. [PR1547540](#)

Documentation Updates

There are no errata or changes in Junos OS Release 21.2R3 documentation for the NFX Series.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 238](#)
- [Basic Procedure for Upgrading to Release 21.2R3 | 239](#)

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 21.2R3, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

NOTE: For information about NFX product compatibility, see [NFX Product Compatibility](#).

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

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

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 11: EOL and EEOL Releases

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

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

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

Basic Procedure for Upgrading to Release 21.2R3

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 21.2R3:

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 | 241](#)
- [What's Changed | 249](#)
- [Known Limitations | 254](#)
- [Open Issues | 254](#)
- [Resolved Issues | 258](#)
- [Documentation Updates | 268](#)
- [Migration, Upgrade, and Downgrade Instructions | 268](#)

These release notes accompany Junos OS Release 21.2R3 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 21.2R3 | 241](#)
- [What's New in 21.2R2 | 241](#)
- [What's New in 21.2R1 | 241](#)

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

What's New in 21.2R3

There are no new features or enhancements to existing features in Junos OS Releases 21.2R3 for PTX Series routers.

What's New in 21.2R2

There are no new features or enhancements to existing features in Junos OS Releases 21.2R2 for PTX Series routers.

What's New in 21.2R1

IN THIS SECTION

- [Hardware | 242](#)
- [High Availability | 243](#)
- [Juniper Extension Toolkit \(JET\) | 243](#)
- [Junos Telemetry Interface | 244](#)
- [Layer 2 VPN | 245](#)

- Network Management and Monitoring | 246
- Routing Options | 246
- Routing Policy and Firewall Filters | 247
- Routing Protocols | 247
- Services Applications | 248
- Source Packet Routing in Networking (SPRING) or Segment Routing | 248

Learn about new features or enhancements to existing features in this release for the PTX Series.

Hardware

- The following methods to protect the chassis from excessive current draw and temperature conditions are supported:
 - Configure Junos OS to automatically shut down the PSM, or raise an alarm and log the event when a field-effect transistor (FET) failure is detected in the power supply module (PSM) by using the specified command. [See [thermal-health-check](#)].
 - Configure upgrade of the PSM firmware that will take action when there is an FET failure by using the specified command. [See [request system firmware upgrade](#)].
 - Configure Junos OS to raise an alarm and log events when a PSM with upgraded firmware version shuts down due to an FET failure, Junos OS on the attached device.
 - Configure a monitor to check how much power the chassis draws from the PSM using the specified command. If the system draws more power from the PSM than what it should consume, Junos OS raises an alarm or shuts down the system. [See [watchdog \(PSM\)](#)]. [See [Handling Thermal Health Events Using Thermal Health Check and PSM Watchdog](#)].
- **Support for AOC transceivers (PTX1000)**—Starting in Junos OS Release 21.2R1, the PTX1000 routers support the following active optical cable (AOC) transceivers:
 - JNP-40G-AOC-1M
 - JNP-40G-AOC-3M
 - JNP-40G-AOC-5M
 - JNP-40G-AOC-7M
 - JNP-40G-AOC-10M

- JNP-40G-AOC-15M
- JNP-40G-AOC-20M
- JNP-40G-AOC-30M

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

High Availability

- **NSR support for RSVP-TE dynamic tunnels (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support nonstop active routing (NSR) for RSVP-Traffic Engineering (RSVP-TE) dynamic tunnels.

[See [Nonstop Active Routing Concepts](#).]

- **NSR support for SR-TE (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support NSR for segment routing-traffic engineering (SR-TE), allowing for hitless traffic flow on Routing Engine switchover. Routes using next hops from SR-TE policies that don't support NSR might experience traffic loss on switchover. The SR-TE policies that don't support NSR are DCSPF and Path Computation Element (PCE).

[See [Segment Routing for Traffic Engineering](#).]

Juniper Extension Toolkit (JET)

- **BGP route service API supports programming routes with IP-IP encapsulation attributes (MX240, MX480, MX960, PTX1000, QFX5110, QFX5200, QFX10002, and QFX10008)**—Starting in Junos OS Release 21.2R1, you can use the BGP route service API to program BGP routes with IP over IP (IP-IP) encapsulation attributes. You can specify the tunnel type, the remote endpoint address, and the color of the route. Keep the following in mind:
 - The egress endpoint must be a unicast IPv4 address.
 - The colors encoded in `tunnel_encap` and `extended_community` must match.
 - If the encapsulation `ext_com` and the tunnel attribute are both present, the egress endpoint must match the next-hop address.

To enable this feature, configure the `bgp-signal` option at the `[edit routing-options dynamic-tunnels tunnel-name]` hierarchy level. The rest of your dynamic tunnel CLI configuration does affect the functionality of the programmed tunnels.

[See [dynamic-tunnels](#) and [JET APIs on Juniper EngNet](#).]

Junos Telemetry Interface

NOTE: For Routing Engine telemetry sensors supported by this platform, see [Telemetry Sensor Explorer](#). If any Platform Forwarding Engine sensors have been added for this release, they are listed below

- **End-of-message notification for Routing Engine sensors (EX2300, EX4300, EX4300-MP, EX9200, MX240, MX960, MX10016, MX2010, MX2020, PTX1000, PTX3000, PTX10001, QFX5100, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we've introduced an end-of-message (EoM) Boolean flag for all Junos telemetry interface (JTI) Routing Engine sensors. The flag notifies the collector that the current wrap has completed for a particular sensor path. A wrap is a complete key-value data dump for all the leaves under a sensor path.

The EoM flag also enables the collector to detect when the end of wrap occurs without having to compare stream creation timestamp values that the collector receives from the packets. Comparing timestamp values is costly time-wise and delays data aggregation.

To use this feature with gRPC Network Management Interface (gNMI) transport or Remote Procedure Call (gRPC), retrieve the protobuf files from the relevant branch on the [Juniper Networks](#) download site:

- GnmJuniperTelemetryHeaderExtension.proto (gNMI)
- agent.proto (for gRPC)

For example: <https://github.com/Juniper/telemetry/blob/master/20.3/20.3R1/protos/GnmJuniperTelemetryHeaderExtension.proto>.

After you download and install the new protobuf files on a collector, the EoM field is present in the packets received.

[See [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **Monitoring and optimizing Packet Forwarding Engine sensor data export (PTX Series and QFX Series)**—Starting in Junos OS Release 21.2R1, you can optimize Packet Forwarding Engine sensor data to dynamically determine how to export data as quickly as possible based on three sensor categories: heavy data (dynamic scale), medium data (predicted scale), and low data (fixed scale). In addition, you can use our new sensor to retrieve export details of all Packet Forwarding Engine sensors. Use the resource path `/junos/system/linecard/export/monitor` to monitor export details for each subscribed Packet Forwarding Engine sensor including:
 - Number of reaps
 - Number of wraps (a complete data set)

- Number of packets sent
- Average number of reaps and wraps
- Timestamps for reaps and wraps

[See [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#) and [Guidelines for gRPC and gNMI Sensors \(Junos Telemetry Interface\)](#).]

- **Enable VOQ utilization monitoring with JTI (PTX1000, PTX5000, PTX10000, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.2R1, you can enable the export utilization data for CoS virtual output queues (VOQs) on aggregated Ethernet or physical Ethernet WAN interfaces. Using this feature, you can export peak buffer utilization data for a given queue with Junos telemetry interface (JTI). Monitoring this data can assist in preventing micro-bursts and high buffer utilization for a given queue because peak buffer utilization is transient and might not be reported by instantaneous queue depth.

To enable monitoring, include `queue-monitoring enable` at one of the following hierarchies:

- [edit class-of-service interfaces *if-name*]
- [edit class-of-service traffic-control-profiles *tcp-name*]
- [edit class-of-service schedulers *scheduler-name*]

To export data to a collector, include the resource path `/junos/system/linecard/qmon-sw` in a subscription.

[See [queue-monitoring](#), [show class-of-service interface](#), [show class-of-service traffic-control-profile](#), [show class-of-service scheduler-map](#) and [show interfaces voq interface-name](#).]

- **JTI: logical interface statistics for IPv4 and IPv6 family input and output counters (MX Series and PTX Series routers using third-generation FPCs)**—Starting in Junos OS Release 21.2R1, you can stream per-family logical interface statistics for IPv4 and IPv6 traffic using Junos telemetry interface (JTI) and Remote Procedure Calls (gRPC) to an outside collector.

To access these sensors, use the resource paths `/junos/system/linecard/interface/logical/family/ipv4/usage/` and `/junos/system/linecard/interface/logical/family/ipv6/usage/` in a subscription.

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

Layer 2 VPN

- **Support for Layer 2 services on SR-TE tunnels using transport class (MX series, PTX Series, and vMX)**—Starting in Junos OS Release 21.2R1, you can configure the following Layer 2 services on colored and non-colored segment routing traffic engineer (SR-TE) tunnels using transport classes.
 - Layer 2 Circuits

- Layer 2 VPN
- BGP VPLS

[See [Layer 2 Circuit Overview](#) ,[Introduction to Configuring Layer 2 VPNs](#), and [BGP Classful Transport Planes Overview](#) .]

Network Management and Monitoring

- **sFlow support for IP-IP traffic with VRF (PTX1000, PTX10002, PTX10008, QFX10002, and QFX10008)**—Starting in Junos OS Release 21.2R1, you can use sFlow technology to sample IP over IP (IP-IP) traffic that is hosted on multiple virtual routing and forwarding (VRF) instances. sFlow sampling now reports the extended router data correctly when the incoming and outgoing interfaces of the traffic reside on two different VRFs in IP-IP traffic for egress sampling.

[See [Overview of sFlow Technology](#).]

- **Support for syslog over TLS (EX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, you can transport syslog (control plane) over Transport Layer Security (TLS) protocol. Encapsulating syslog over 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
- 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.

Routing Options

- **Enhancements to prefix-limit and accepted-prefix-limit configuration statements, and updates to show bgp neighbor command (ACX1000, EX9200, MX Series, PTX5000, and QFX10002)**— Starting from Junos OS Release 21.2R1, the `prefix-limit` and `accepted-prefix-limit` configuration statements include the following options:

- `drop-excess <percentage>`—If you include the `drop-excess <percentage>` option, the excess routes are dropped when the maximum number of prefixes is reached. If you specify a percentage, the routes are logged when the number of prefixes exceeds that percentage value of the maximum number.
- `hide-excess <percentage>`—If you include the `hide-excess <percentage>` option, the excess routes are hidden when the maximum number of prefixes is reached. If you specify a percentage, the routes are logged when the number of prefixes exceeds that percentage value of the maximum number.

The `show bgp neighbor` command has been enhanced to display the following additional information:

- Count of prefixes that are dropped or hidden based on network layer reachability information (NLRI) when the maximum allowed prefixes threshold is exceeded.
- Alerts when a peer starts to drop or hide routes.
- Configuration details of the `prefix-limit` and `accepted-prefix-limit` configuration statements.

[See [prefix-limit](#), [accepted-prefix-limit](#), [show bgp neighbor](#), and [Multiprotocol BGP](#).]

Routing Policy and Firewall Filters

- **Class-based firewall filters (PTX Series)**—Starting in Junos OS Release 21.2R1, you can apply firewall filter actions like drop, reject, sample, and police on packets classified by destination class usage (DCU) and source class usage (SCU) accounting, for example as part of a design to provide distributed denial-of-service (DDoS) protection to specific customers.

[See [Configuring the Filter Profile](#).]

Routing Protocols

- **Support for origin validation with BGP sharding (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, you can use origin validation with BGP sharding. You can configure `rib-sharding` with `routing-options validation`.
- **BMP with BGP sharding and update I/O (JRR Series, MX Series, PTX Series, and vMX)**—Starting in Junos OS Release 21.2R1, we support BGP Monitoring Protocol (BMP) with BGP sharding and update I/O in the multithreaded mode.
- **Basic MVPN support with BGP sharding (cRPD, JRR200, MX2020, PTX5000, and QFX10002)**—Starting in Junos OS 21.2R1, we support the basic multicast virtual private network (MVPN) functionalities with BGP sharding.

NOTE: Sharding is not supported for the MVPN address family.

- **Support for BGP SR-TE policy advertisement and error handling (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, if the SDN controller cannot directly install SR-TE routes on non-Juniper Networks devices, the controller installs the BGP SR-TE policy on the route reflector, which forwards the SR-TE routes to non-Juniper devices.

To advertise SR-TE policy to non-Juniper devices, define a BGP policy that includes the family `inet-srte` statement at the `[edit policy-options policy-statement term from protocol bgp]` hierarchy level.

To push an unlabeled IP packet before other labels, include the `inet-color-append-explicit-null` statement at the `[edit protocols source-packet-routing]` hierarchy level.

- **Support for BGP classful transport (CT) with underlying colored SRTE tunnels (MX Series and PTX Series with FPC-PTX-P1-A)**— Starting in Junos OS Release 21.2R1, BGP-CT can resolve service routes using the transport RIBs and compute the next-hop. Services currently supported over BGP-CT can also use the underlying SRTE colored tunnels for route resolution.

To enable BGP CT service route resolution over underlying SRTE colored tunnels, include the `use-transport-class` statement at the `[edit protocols source-packet-routing]` hierarchy level.

[See [use-transport-class](#).]

- **Flexible algorithm inter-level leaking support for SRv6 and SR-MPLS in ISIS (ACX Series, MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support flexible algorithm inter-level leaking for SRv6 and SR-MPLS in IS-IS. Also, we partially support TE-App RFC 8919 in its basic form and extends 6PE support for flexible algorithm.

Services Applications

- **Support for hardware timestamping of Two-Way Active Measurement Protocol (TWAMP) and RPM probe messages (PTX5000)**—Starting in Junos OS Release 21.2R1, we've extended support for hardware timestamping of TWAMP and RPM probe messages. Hardware timestamping is enabled by default for TWAMP, but you must configure it for RPM. You use TWAMP and RPM to measure IP performance between two devices in a network. By configuring hardware timestamping for RPM, you can account for the latency in the communication of probe messages and generate more accurate timers in the Packet Forwarding Engine. To configure hardware timestamping for RPM, include the `hardware-timestamping` statement at the `[edit services rpm probe probe-owner test test-name]` hierarchy level.

[See [Understanding Two-Way Active Measurement Protocol on Routers](#), [Understanding Using Probes for Real-Time Performance Monitoring on M, T, PTX, and MX Series Routers](#), and [Configuring RPM Timestamping on MX, M, T, and PTX Series Routers and EX Series Switches](#).]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Static route resolution over SR-TE tunnel (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support static route resolution over segment routing-traffic engineered (SR-TE) colored

and uncolored label-switched paths (LSPs). To enable this feature, configure the `spring-te-lsp-next-hop` statement at the `[edit routing-options static destination]` and `[edit routing-options rib rib name static destination]` hierarchy levels. The feature support extends towards static, DTM, BGP-SR-TE, and PCEP source types that are currently supported by Source Packet Routing in Networking–Traffic Engineering (SPRING-TE). If a source is not configured, by default, it takes the next hop as static.

You must configure the `tunnel-tracking` statement at the `[edit protocols source-packet-routing]` hierarchy level to enable this feature. This feature enhances the accuracy of first-hop label-based tunnel status for SR-TE tunnels according to their route resolution.

[See [spring-te-lsp-next-hop](#) and [source-packet-routing](#).]

- **Express segments using SR-TE underlay (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we've introduced SR-TE underlay path support for express segments to enable end-to-end transport of segment routing–traffic engineered (SR-TE) label-switched paths (LSPs) for very large multi-domain networks. The path is automated using `segment-set` or `template` policies for uncolored or colored segment routing policies. The `rib-group` configuration is required to import addresses to `inet.3` for colored segment routing policies. When the express segments underlay is colored SR-TE, you need to configure the `no-chained-composite-next-hop` statement at the `[edit protocols source-packet-routing]` hierarchy level for the express segment to install the correct flattened next hop.

This feature has the following limitations:

- When the express segments underlay is colored SR-TE, the express segment does not inherit the SR-TE LSP underlay attributes (SR-TE name, metric).
- The `install-nexthop` option at the `[edit policy-options policy-statement policy-name term term-name then]` hierarchy level to filter a specific SR-TE LSP by its name is not supported.
- Express segments do not consider the respective weights of the primary and secondary segment lists of SR-TE LSP. Secondary LSP segments can be preferred for traffic even when the primary segment is up.

[See [Express Segment LSP Configuration](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 250](#)
- [What's Changed in Release 21.2R2 | 250](#)

- [What's Changed in Release 21.2R1 | 251](#)

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

What's Changed in Release 21.2R3

IN THIS SECTION

- [Network Management and Monitoring | 250](#)

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.](#)]
- **Changes to the NETCONF `<edit-config>` RPC response (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<edit-config>` operation returns an error, the NETCONF server does not emit a `<load-error-count>` element in the RPC response. In earlier releases, the `<edit-config>` RPC response includes the `<load-error-count>` element when the operation fails.

What's Changed in Release 21.2R2

There are no changes in behavior and syntax in Junos OS Releases 21.2R2 for PTX Series routers.

What's Changed in Release 21.2R1

IN THIS SECTION

- [Class of Service \(CoS\) | 251](#)
- [EVPN | 251](#)
- [General Routing | 251](#)
- [Interfaces and Chassis | 252](#)
- [Junos XML API and Scripting | 252](#)
- [Network Management and Monitoring | 253](#)

Class of Service (CoS)

- Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

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

- **SSH session connection limit and rate limit per connection (PTX Series and QFX Series)**— We have introduced SSH `connection-limit` and `rate-limit` options at the `[edit system services ssh]` hierarchy levels to enable SSH connection limit and rate limit per connection. The default connection limit value is 75 connections and there is no default value associated with rate limit.
- **Secure boot disabled alarm is raised (PTX10008)**— The `Secure boot disabled` alarm is raised when the system boots with secure boot disabled in bios.
- **Enhancement to the show chassis pic command (Junos OS)**—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 ae interfaces. You can now view following additional fields for MAC statistics : Receive, Transmit, Broadcast and Multicast packets.

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

Interfaces and Chassis

- **Blocking duplicate IP detection in the same routing instance (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, and SRX Series)**—Junos will no longer accept duplicate IPs between different logical interfaces in the same routing instance. Refer to the table mentioned in the topic `inet (interfaces)`. When you try to configure same IP on two logical interfaces inside same routing instance, the commit will be blocked with the error displayed as shown below:

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.2/24
[edit]
user@host# commit
commit complete
[edit]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 2.2.2.2/24
[edit]
user@host# commit
[edit interfaces ge-0/0/2 unit 0 family inet]
'address 2.2.2.2/24'
identical local address found on rt_inst [default], intfs [ge-0/0/2.0 and ge-0/0/1.0],
family [inet].
error: configuration check-out failed
```

[See [inet\(interfaces\)](#).]

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.](#)]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See [request system scripts refresh-from](#) and [cert-file \(Scripts\)](#).]

Network Management and Monitoring

- **Chef and Puppet support removed (EX Series except EX4400, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, Junos OS products that were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS. FreeBSD 12.x based Junos OS does not support installing existing Chef or Puppet packages.
- **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.](#)]

- **Changes to <commit> RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server's response for <commit> operations includes the following changes:
 - If a successful <commit> operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.

- The NETCONF server response emits the `<source-daemon>` element as a child of the `<error-info>` element instead of the `<rpc-error>` element.
- If you also configure the `flatten-commit-results` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server suppresses any `<commit-results>` XML subtree in the response and only emits an `<ok/>` or `<rpc-error>` element.

[See [Configuring RFC-Compliant NETCONF Sessions.](#)]

Known Limitations

IN THIS SECTION

- [Infrastructure | 254](#)

Learn about known limitations in Junos OS Release 21.2R3 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.

Infrastructure

- When upgrading from before Junos OS Release 21.2 to 21.2 and after, validation and upgrade will fail. The upgrading requires using of `no-validate` configuration. [PR1568757](#)

Open Issues

IN THIS SECTION

- [General Routing | 255](#)
- [Layer 2 Ethernet Services | 256](#)

- [MPLS | 256](#)
- [Routing Protocols | 257](#)
- [User Interface and Configuration | 257](#)

Learn about open issues Junos OS Release 21.2R3 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 PTX platforms, some non-fatal interrupts (for example, CM cache or AQD interrupts) are logged as fatal interrupts. The following log messages will be shown on CM parity interrupt: fpc0 TQCHIP 0: CM parity Fatal interrupt,Interrupt status:0x10 fpc0 CMSNG: Fatal ASIC error, chip TQ fpc0 TQCHIP 0: CM cache parity Fatal interrupt has occurred 181 time(s) in 180010 msec TQCHIP 0: CM cache parity Fatal interrupt has occurred 181 time(s) in 180005 msec. [PR1089955](#)
- On a PTX Series router or QFX10000 switch with a third-generation FPC, an error message is displayed when the FPC goes online or offline. [PR1322491](#)
- Due to transient hardware condition, single-bit error (SBE) events are corrected and have no operational impact. Reporting of those events had been disabled to prevent alarms and possibly unnecessary hardware replacements. This change applies to all Platforms using Hybrid Memory Controller (HMC). [PR1384435](#)
- This is a timing issue during the sxe interface bring up (w.r.t i40e driver). This can be recovered by rebooting the complete board. [PR1442249](#)
- On Junos PTX and 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](#)
- On the PTX platforms with NG-RE installed, after upgrading the Intel i40e-NVM firmware to version 6.01, the FRUs disconnection alarms might be seen along with traffic loss. Please refer to the TSB17603 (<https://kb.juniper.net/TSB17603>) to upgrade Junos software and Intel i40e-NVM firmware. [PR1529710](#)
- FIPS mode is not supported. [PR1530951](#)
- 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 platforms, when Inline Jflow is configured and high sampling rate (more than 4000 per second) is set, high CPU utilization may be observed and this might result in relevant impacts on traffic analysis and billing. [PR1569229](#)
- Copying files to /tmp/ causes a huge JTASK_SCHED_SLIP. Copy files to /var/tmp/ instead. [PR1571214](#)
- On PTX10008, the end-to-end traffic is not flowing for ethernet-switching in EP style. [PR1583219](#)
- 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 hold-time for up and down helps to resolve. [PR1601946](#)
- Under MAC statistics **output-mac-control-frames** & **output-mac-pause-frames** does not increase. [PR1610745](#)
-
- While loading baseline configurations in PTX5000 box, continuous FPC core seen at pci_user_pio_read_func and posix_interface_abort along with scheduler hog messages. [PR1644576](#)
- PTX10008 mgmt interface em0 shows speed as 10G instead of 1G. [PR1642731](#)

Layer 2 Ethernet Services

- If **request system zeroize** does not trigger zero-touch provisioning, please re-initiate the ZTP as a workaround. [PR1529246](#)

MPLS

- As the update-threshold configuration changes from an attribute to an object, you need to delete the update-threshold stanza and re-configure it after the downgrade. [PR1546447](#)
- The RSVP interface update threshold configuration syntax has changed between Junos OS Release 18.2X75-D435 and Junos OS Release 20.3X75-D10 to include curly braces around the threshold

value. Upgrading and downgrading between these releases is not entirely automatic. The user must delete this stanza if configured before the downgrade and then manually reconfigure. [PR1554744](#)

- On PTX3000 platform, if RPD thrashes during a GRES switchover, there might be traffic loss on MPLS LSPs. [PR1590681](#)

Routing Protocols

- Due to a race condition between route re-convergence and the BGP-PIC version up message to the Packet Forwarding Engine, after a remote transit router reboot, certain BGP routes might reuse stale LDP next hops and cause packet discard at the transit router during the route re-convergence window. [PR1495435](#)
- If OSPF and RSVP are configured, when a device that is out of service is transmitting a large number of LSAs (more than 100,000), extremely busy neighbors are slow in sending LSACKs, and some LSA churn happens caused by route flaps. Then unexpected CSPF link down/deleted events happen on LSPs. This causes other OSPF routers in the OSPF domain to fail their CSPF calculation for the router loopbacks that act as P routers in this topology and thus drop the LSPs, causing traffic impairment. In addition, rpd utilization will be pegged to 100%. [PR1576818](#)
- Traffic loss across the LDP path during traffic shift to another device in the MPLS cloud. Here two routers with two different capacities are converging at two different times, so the micro loop occurs between the two nodes. [PR1577458](#)
- On all Junos and EVO platforms, traffic might continue to forward on the AE (aggregated Ethernet) member link even if MicroBFD (Bidirectional Forwarding Detection) status is in a hold-down state. There is no traffic loss due to the issue. [PR1624085](#)

User Interface and Configuration

- On PTX platforms, the default routing policy might not be changed back after it is changed to network-services enhanced mode. [PR1587174](#)
- On all Junos OS platforms, when copy-configuration, get-configuration, discard-change RPCs run in two parallel NETCONF sessions and the database is also accessed in parallel by two NETCONF sessions, it leads to database corruption and mgd related services might crash. [PR1641025](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.2R3 | 258](#)
- [Resolved Issues: 21.2R2 | 261](#)
- [Resolved Issues: 21.2R1 | 263](#)

Learn about 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: 21.2R3

IN THIS SECTION

- [General Routing | 258](#)
- [Juniper Extension Toolkit \(JET\) | 260](#)
- [Layer 2 Ethernet Services | 260](#)
- [MPLS | 260](#)
- [Platform and Infrastructure | 260](#)
- [Routing Policy and Firewall Filters | 260](#)
- [Routing Protocols | 260](#)
- [User Interface and Configuration | 260](#)

General Routing

- High FPC CPU utilization might be seen on PTX10002-60C platform. [PR1585728](#)
- IS-IS adjacency is not coming up through TCC I2circuit. [PR1590387](#)
- On PTX10001-36MR, inconsistency in the platform name used in multiple places, version, snmp mibs, etc. [PR1597999](#)

- On PTX10004, EVPN-VXLAN shared tunnel configuration need to be removed. [PR1598142](#)
- CRC errors increase continuously after interface flap. [PR1600768](#)
- On Junos OS PTX10002-60C device, after upgrading, configured firewall filters might be applied on incorrect interfaces (CVE-2021-31382). [PR1602292](#)
- FPC is not fully offline after FPC BAD_VOLTAGE fault is reported. [PR1602556](#)
- Traffic loss might be seen on the device due to the continuous errors happening on Fabric Healing process (FHP) phase-1. [PR1603499](#)
- Link flaps might be observed momentarily on PTX5000 platforms. [PR1606008](#)
- 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 rasdaemon processes memory leak -- triggered by hardware memory errors on VMHost platforms. [PR1615488](#)
- 90% traffic got dropped when the number of Switch Interface Board (SIB) plane is reduced from 4 to 3 on PTX10008 and PTX10016. [PR1615942](#)
- Slow memory leak (32 bytes each time) of rpd might be seen [PR1616065](#)
- Layer 2 cpd memory leak might lead to l2cpd process crash. [PR1617151](#)
- Unexpected Routing Engine switchover might be observed. [PR1617720](#)
- Performance of Jflow service might be impacted on PTX platforms. [PR1617932](#)
- Traffic loss might be observed with some MPLS labels in multipath BGP scenarios. [PR1618507](#)
- PTX sflow server log does not contain srcIP and desIP details. [PR1620140](#)
- EAPoL packets over l2circuit might get dropped at the tunnel start. [PR1628196](#)
- SNMP trap message for fpc restart, shows as FRU removal instead of Fru Offline/Fru Power off. [PR1629738](#)
- Multiple link flaps and traffic might be lost on the links. [PR1630006](#)
- RPD core might be observed with warm-standby configurations due to reference counting issues. [PR1631871](#)
- SPMB might crash immediately after a switchover. [PR1637950](#)

Juniper Extension Toolkit (JET)

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

Layer 2 Ethernet Services

- BFD hold-down timer does not work properly when LAG is configured. [PR1616764](#)
- The aggregated Ethernet interface remains UP instead of down on deleting loopback and aggregated Ethernet interface IP on neighbor while verifying BFD sessions on router. [PR1640240](#)

MPLS

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

Platform and Infrastructure

- On PTX platforms vmcore on both the Routing Engines might be reported due to mbuf corruption. [PR1602442](#)

Routing Policy and Firewall Filters

- BGP import policy is not applied to all the routes when CCNH inet is enabled. [PR1596436](#)

Routing Protocols

- The rpd might crash in BGP multipath scenario if interface for a single hop EBGP peer goes down. [PR1589141](#)
- Delay in adding and removing static routes from the router. [PR1612173](#)
- Undesired protection path might get selected for some destination prefixes. [PR1614683](#)
- The rpd might crash and restart when NSR is enabled. [PR1620463](#)
- The rpd might crash after clearing IS-IS database. [PR1631738](#)

User Interface and Configuration

- The core files can not be deleted using CLI file delete /var/core/*/vmcore*. [PR1624562](#)

Resolved Issues: 21.2R2

IN THIS SECTION

- [General Routing | 261](#)
- [Interfaces and Chassis | 262](#)
- [MPLS | 262](#)
- [Multicast | 262](#)
- [Network Management and Monitoring | 262](#)
- [Platform and Infrastructure | 263](#)
- [Routing Protocols | 263](#)

General Routing

- Upgrading the PTX1000 devices with unified SSDs (2x32G SSD) might result in a boot loop in certain scenario. [PR1571275](#)
- Mirrored packets get corrupted when you apply filter with action port-mirror and then discard. [PR1576914](#)
- The **RPD_KRT_KERNEL_BAD_ROUTE** error message is seen in certain scenarios when the rpd process restarts or GRES happens when NSR is enabled. This error has no functional impact. [PR1586466](#)
- The na-grpc process crash might be seen and existing telemetry connections will be disconnected. [PR1587956](#)
- In a telemetry scenario, the jsd process crash might be seen in rare situations. [PR1589103](#)
- Traffic loss might be observed after changing SAK keys. [PR1591432](#)
- The l2cpd-agent might go unresponsive after starting telemetry service. [PR1592473](#)
- On PTX10008 and PTX10001-36MR platforms, sflow sample-rate configuration greater than 16000000 is not supported. [PR1592788](#)
- [MPC10E] messages log will be filled with **Temp Sensor Fail** alarm set or clear and **cmtfpc_cpu_core_temp_get: Fail to get temp CPU7_PMB** messages. [PR1597798](#)
- On PTX10001-36MR, inconsistency in the platform name used in multiple places, version, snmp mibs, etc. [PR1597999](#)

- [sflow] [sflow_sample] PTX1000 :: JDI_FT_REGRESSION:PLATFORM_PFE:ROUTING:Longrow: Longrow [PTX1000]:sflow: Sflow data (inner vlan and outer vlan value, forwarding-class, DSCP value) is not exported while checking from server flow-records at the collector for Ingress Sampling. [PR1598263](#)
- Traffic blackhole might be seen due to the **RS Fatal** error on FPC-PTX-P1-A/FPC2-PTX-P1A/FPC-SFF-PTX-P1-A/FPC-SFF-PTX-T. [PR1600935](#)
- The Layer 2 circuit packets with destination mac 01:00:0c:cc:cc:cd might get punted. [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](#)
- On PTX5000 router, link might flap momentarily. [PR1606008](#)
- Memory leaks might be observed on the l2cpd process when performing certain LLDP operations. [PR1608699](#)
- Line-cards might be unstable due to the continuous growing memory usage of evo-cda-bt app. [PR1614952](#)
- The node name must not be attached to the system hostname under LLDP. [PR1593991](#)

Interfaces and Chassis

- The Junos Telemetry Interface optics sensor's alarm data type changed from **bool_val** to **str_val**. [PR1580113](#)

MPLS

- The LDP replication session might not get synchronized when the dual-transport statement is enabled. [PR1598174](#)
- VPLS connection might get down if the dual-transport statement is configured. [PR1601854](#)

Multicast

- Multicast traffic in MVPN setup might be silently dropped and discarded on 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

- In 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 Protocols

- 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](#)

Resolved Issues: 21.2R1

IN THIS SECTION

- [General Routing | 263](#)
- [EVPN | 266](#)
- [Forwarding and Sampling | 266](#)
- [General Routing | 266](#)
- [Infrastructure | 266](#)
- [Layer 2 Ethernet Services | 266](#)
- [MPLS | 266](#)
- [Multicast | 267](#)
- [Network Management and Monitoring | 267](#)
- [Routing Policy and Firewall Filters | 267](#)
- [Routing Protocols | 267](#)
- [User Interface and Configuration | 267](#)
- [VPNs | 268](#)

General Routing

- FPC reboot might be observed in the events of jlock hog more than 5 seconds. [PR1439929](#)
- The dcufe crash might be seen on platforms with auto-channelization enabled. [PR1484336](#)
- Aggregate Ethernet interfaces do not display member links' statistic. [PR1505596](#)

- Error messages `t6e_dfe_tuning_state:et-6/0/0` - Failed to dfe tuning count 10 might be seen after links flap [PR1512919](#)
- Packet drops might be seen with all commit events with 1G speed configured interface. [PR1524614](#)
- The VM host platform might crash continuously after performing upgrade or downgrade and booting up with the new image. [PR1544875](#)
- On the PTX10000 platforms, traffic might get dropped when the set routing-options forwarding-table no-ecmp-fast-reroute configuration is changed to 128 ECMP entries. [PR1547457](#)
- WR Linux 6 platforms might get stuck after upgrading or downgrading image version and restarting device. [PR1547669](#)
- PTX1000 and PTX10002 platforms could get stuck after performing vmhost reboot post image upgrade. [PR1548254](#)
- On PTX3000 platform, the chassisd might crash with faulty SIB3. [PR1551291](#)
- The interface filter with source-port 0 matches everything instead of port 0. [PR1551305](#)
- Packet drop might happen on the aggregate Ethernet bundle which has the single child member only. [PR1551736](#)
- There might be traffic drop when default EXP classifier maps traffic to FC with no schedulers. [PR1554266](#)
- The micro BFD session might flap with DDoS policer. [PR1557782](#)
- The device might run out of service post GRES/ISSU. [PR1558958](#)
- Major alarms might be seen when a large class-of-service buffer-size is configured. [PR1559459](#)
- Traffic drop might be seen in 128 or more way ECMP paths after FPC restart. [PR1559528](#)
- The command `show system health-monitor` is hidden for PTX10000 platform. [PR1560268](#)
- In PTX10000 platform, the command `set chassis display` is hidden. [PR1560453](#)
- After recovering from restart routing immediately, object-info anomalies are observed on rpdagent. [PR1561812](#)
- On PTX10000, an enhancement to enable watchdog petting log on Line Cards. [PR1561980](#)
- The dcpfe process might crash in ECMP scenario. [PR1564147](#)
- Junos OS, upon receipt of specific packets BFD sessions might flap due to DDoS policer implementation in Packet Forwarding Engine (CVE-2021-0280). [PR1564807](#)

- On PTX10002-60C platform, another port will also shutdown after shutting down one port. [PR1568294](#)
- LLDP out-of-bounds read vulnerability in l2cpd. [PR1569312](#)
- Interface hold-time down feature might not work in certain conditions. [PR1570204](#)
- PTX1000 with unified disk fails netboot with Timed out waiting for device dev-jvg_P-jlvmjunos.device message. [PR1571275](#)
- The gRPC session hanging is in CLOSED state. [PR1571999](#)
- Channelized ports on PTX10002 platforms might drop traffic. [PR1575742](#)
- In PTX5000, you might observe traffic loss. [PR1578511](#)
- TACACS traffic might be dropped. [PR1578579](#)
- BFD sessions might flap during traffic spikes on PTX platforms. [PR1578599](#)
- Authentication might fail if the password contains special characters. [PR1580003](#)
- The IS-IS packet might be corrupted on the provider edge device over the Layer 2 circuit tunnel. [PR1580047](#)
- On PTX platforms, the traffic might drop. [PR1580211](#)
- The clear synchronous-ethernet wait-to-restore interface command not available. [PR1581556](#)
- On PTX5000 and PTX3000, configure and delete the FEC mode will disable the auto-FEC91 on an interface that uses QSFP28-SR4. [PR1582200](#)
- Junos telemetry Interfaces: Missing Leaves - Transceiver/state. [PR1583076](#)
- On PTX10008, show chassis clocks - should be handled in a meaningful error. [PR1583715](#)
- The packets might be dropped by Packet Forwarding Engine of PTX5000 after changing the queue of IEEE-802.1ad classifier on FPC-PTX-P1-A or FPC2-PTX-P1A. [PR1584042](#)
- On Junos OS, QFX Series and PTX Series; FPC resource usage increases when certain packets are processed which are being VXLAN encapsulated (CVE-2021-31361). [PR1584197](#)
- JDI-RCT: T/PTX, 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 seen during bringup. [PR1585594](#)
- The na-grpc process crash might be seen and existing telemetry connections will be disconnected. [PR1587956](#)
- There might be higher latency in traffic flow than configured or default value. [PR1588514](#)

- In a telemetry scenario, the jsd process crash might be seen in rare situations. [PR1589103](#)
- On PTX3000 and PTX5000 platforms, the 40G and 100G interface might get stuck down after link flaps. [PR1589170](#)
- The Layer 2 circuit packets with destination mac 01:00:0c:cc:cc:cd may get punted. [PR1601360](#)

EVPN

- EVPN option is missing under [edit routing-instances routing-instance-name protocols] [PR1581821](#)

Forwarding and Sampling

- Junos OS, user-defined ARP Policer is not applied on Aggregated Ethernet (AE) interface until firewall process is restarted (CVE-2021-0289). [PR1528403](#)

General Routing

- On PTX10008, NSR Support for LDP/RSVP/BGP: BGP NH_index (indirect and unilist) change after GRES+NSR Trigger causing a momentary (unexpected) traffic loss. [PR1560323](#)

Infrastructure

- The kernel crash with core file might be seen if churn happens for a flood composite next hop. [PR1548545](#)
- The TCP session might fail on devices with dual Routing Engines. [PR1555441](#)
- Next-hop incorrectly associated with lo0 in forwarding-table when interface is configured as unnumbered. [PR1570918](#)

Layer 2 Ethernet Services

- The copying of files to the RCB over WAN ports is slow. [PR1496895](#)

MPLS

- MPLS-LIB memory leak might be seen in SR scenario. [PR1556495](#)
- Traffic sent over an LSP might be dropped if two consecutive PLRs along the LSP perform local repair and bypass protecting the second PLR fails. [PR1566101](#)

- The rpd process on the transit node might crash when MPLS traceroute on the ingress node is performed. [PR1573517](#)
- Sub-optimal routing issues might be seen in case LDP route with multiple next-hops. [PR1582037](#)

Multicast

- FPC might crash in a multicast scenario. [PR1569957](#)

Network Management and Monitoring

- The mib2d process crashes and generates a core dump on backup Routing Engine. [PR1557384](#)
- FPC crash might be observed in a scaled firewall configuration on PTX series platforms. [PR1586817](#)

Routing Policy and Firewall Filters

- Generated route goes to the hidden state when the protect core command is enabled. [PR1562867](#)

Routing Protocols

- The rpd might restart after interface flap if Layer2-map. [PR1557710](#)
- BGP LU session flap might be seen with the AIGP used scenario. [PR1558102](#)
- Traffic loss might occur for stitched traffic from SR towards LDP if no-eligible-backup is configured. [PR1558565](#)
- The ppm memory leak might cause traffic loss. [PR1561850](#)
- Traffic loss might be observed due to the rpd crash in BGP multipath scenario. [PR1568600](#)
- BGP session carrying VPNv4 prefix with IPv6 next-hop might be dropped. [PR1580578](#)
- Process rpd crash might be seen in certain IS-IS scenario. [PR1583484](#)
- The rpd crash might be seen when BGP RPKI session record-lifetime is configured less than the hold-time. [PR1585321](#)
- BGP Egress-TE routes lose to BGP routes using the same protocol-preference. [PR1593332](#)

User Interface and Configuration

- The LACP might stop working after disabling LACP sync-reset. [PR1576146](#)

VPNs

- The rpd might crash during a race condition under BGP multipath scenario. [PR1567918](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.2R3 documentation for PTX Series routers.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading to Release 21.2 | 268](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 271](#)
- [Upgrading a Router with Redundant Routing Engines | 272](#)

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 21.2R3, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

Basic Procedure for Upgrading to Release 21.2

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

NOTE: 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 21.2R3:

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-
x86-64-21.2R3.9.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-
x86-64-21.2R3.9-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 21.2 `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 12: EOL and EEOL Releases

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

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

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

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 | 273](#)
- [What's Changed | 285](#)
- [Known Limitations | 290](#)
- [Open Issues | 292](#)
- [Resolved Issues | 299](#)
- [Documentation Updates | 320](#)
- [Migration, Upgrade, and Downgrade Instructions | 320](#)

These release notes accompany Junos OS Release 21.2R3 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 21.2R3 | 274](#)
- [What's New in 21.2R2 | 274](#)
- [What's New in 21.2R1 | 277](#)

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

What's New in 21.2R3

There are no new features or enhancements to existing features for QFX Series in Junos OS Release 21.2R3.

What's New in 21.2R2

IN THIS SECTION

- [EVPN | 274](#)
- [Additional Features | 276](#)

Learn about new features or enhancements to existing features in this release for the QFX Series.

EVPN

- **EVPN-VXLAN fabric with an IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.2R2, you can configure an EVPN-VXLAN fabric with an IPv6 underlay. You can use this feature only with MAC-VRF routing instances (all service types). You must configure either an IPv4 or an IPv6 underlay across the EVPN instances in the fabric; you can't mix IPv4 and IPv6 underlays in the same fabric.

To enable this feature, include these steps when you configure the EVPN underlay:

- Configure the underlay VXLAN tunnel endpoint (VTEP) source interface as an IPv6 address:

```
set routing-instances mac-vrf-instance-name vtep-source-interface lo0.0 inet6
```

- Even though the underlay uses the IPv6 address family, for BGP handshaking to work in the underlay, you must configure the router ID in the routing instance with an IPv4 address:

```
set routing-instances mac-vrf-instance-name routing-options router-id ipv4-address
```

- Enable the Broadcom VXLAN flexible flow feature, which is required in Junos OS Release 21.2R2 where the feature is not enabled by default:

```
set forwarding-options vxlan-flexflow
```


We support the following EVPN-VXLAN features with an IPv6 underlay:

- EVPN Type 1, Type 2, Type 3, Type 4, and Type 5 routes. [See [EVPN Type-5 Route with VXLAN Encapsulation for EVPN-VXLAN](#).]
- Shared VTEP tunnels (required with MAC-VRF instances).
- All-active multihoming. [See [EVPN Multihoming Overview](#).]
- EVPN core isolation. [See [Understanding When to Disable EVPN-VXLAN Core Isolation](#).]
- Bridged overlays. [See [Bridged Overlay Design and Implementation](#).]
- Layer 3 gateway functions in ERB and CRB overlays with IPv4 or IPv6 traffic.
- Underlay and overlay load balancing.
- Layer 3 protocols over IRB interfaces—BFD, BGP, OSPF. [See [Supported Protocols on an IRB Interface in EVPN-VXLAN](#).]
- Data center interconnect (DCI)—over-the-top (OTT) full mesh only. [See [Over-the-Top Data Center Interconnect in an EVPN Network](#).]
- EVPN proxy ARP and ARP suppression, and proxy NDP and NDP suppression. [See [EVPN Proxy ARP and ARP Suppression, and Proxy NDP and NDP Suppression](#).]

See [Understanding EVPN with VXLAN Data Plane Encapsulation](#) and [EVPN User Guide](#).

- **DHCP relay in an EVPN-VXLAN fabric with an IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.2R2, EVPN-VXLAN fabrics with an IPv6 underlay support DHCP relay. You can configure the DHCP relay agent in centrally routed and edge-routed bridging overlays. Support for DHCP relay includes DHCPv4 and DHCPv6.
- **Port mirroring and analyzers in an EVPN-VXLAN fabric with an IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y)**—Starting in Junos OS Release 21.2R2, you can configure port mirroring and analyzers on QFX5120 switches in an EVPN-VXLAN fabric with an IPv6 underlay. Port mirroring sends copies of all packets or policy-based sample packets to local or remote analyzers where you can monitor and analyze the data.

[See [Port Mirroring and Analyzers](#).]

- **Support for storm control, MAC filtering, and BPDU protection in EVPN-VXLAN with IPv6 underlay (QFX5120)**—Starting in Junos OS Release 21.2R2, QFX5120 switches set up for EVPN-VXLAN with an IPv6 underlay support storm control for ingress traffic on Ethernet switching interfaces that are part of the EVPN-VXLAN instance. These switches also support bridge protocol data units (BPDUs) and user-defined profiles for broadcast, unknown unicast, and multicast (BUM) traffic. Firewall filter-

based MAC filtering is also supported with the following match conditions: source and destination MAC addresses, source and destination ports, user VLAN ID, EtherType, and IP protocol.

[See [MAC Filtering, Storm Control, and Port Mirroring Support in an EVPN-VXLAN Environment.](#)]

- **Support for firewall filters on EVPN-VXLAN with IPv6 underlays (QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos Release 21.2R2, QFX5120 switches support firewall filters for ingress and egress traffic on EVPN-VXLAN with IPv6 underlays.

[See [Understanding EVPN with VXLAN Data Plane Encapsulation.](#)]

- **Seamless EVPN-VXLAN stitching with MAC-VRF routing instances (QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.2R2, 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.](#)]

- **sFlow support for EVPN-VXLAN with IPv6 underlay (QFX5120-32C, QFX5120-48T, and QFX5120-48Y)**—Starting in Junos OS Release 21.2R2, QFX5120 switches support sFlow monitoring technology to sample traffic on EVPN-VXLAN with an IPv6 underlay.

[See [EVPN-VXLAN Support for VXLAN Underlay](#) and [Overview of sFlow Technology.](#)]

- **CoS support for EVPN-VXLAN with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.2R2, you can configure CoS features, which enable you to prioritize traffic, on an EVPN-VXLAN fabric with an IPv6 underlay.

[See [CoS Support on EVPN VXLANs.](#)]

Additional Features

Support for the following features has been extended to these platforms.

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

[See [interconnect.](#)]

- **sFlow support for EVPN-VXLAN with IPv4 underlay** (QFX10002-60C, QFX10002, QFX10008, and QFX10016)

[See [EVPN-VXLAN Support for VXLAN Underlay](#) and [Overview of sFlow Technology](#).]

What's New in 21.2R1

IN THIS SECTION

- [Dynamic Host Configuration Protocol | 277](#)
- [EVPN | 278](#)
- [Forwarding Options | 279](#)
- [High Availability | 279](#)
- [Interfaces | 279](#)
- [Juniper Extension Toolkit \(JET\) | 280](#)
- [Junos Telemetry Interface | 280](#)
- [Licensing | 282](#)
- [Network Management and Monitoring | 283](#)
- [Routing Options | 284](#)
- [Routing Protocols | 284](#)
- [Services Applications | 284](#)
- [Software Installation and Upgrade | 285](#)
- [System Management | 285](#)

Learn about new features or enhancements to existing features in this release for the QFX Series.

Dynamic Host Configuration Protocol

- **Relay agent information options for stateless DHCP relay (QFX Series)**—Starting in Junos OS Release 21.2R1, QFX Series switches support the configuration of relay agent information options for stateless DHCP relay. These options enable the relay agent to add information to DHCP client requests that the relay agent forwards to the DHCP server. The remote ID and circuit ID options are supported for both DHCPv4 and DHCPv6 stateless relay.

[See [DHCP Relay Agent](#).]

EVPN

- **EVPN Type 2 and Type 5 route coexistence (EX4650, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we support the coexistence of EVPN Type 2 and Type 5 routes in EVPN-VXLAN edge-routed bridging overlay fabrics. This feature enables more efficient traffic flow and better usage of Packet Forwarding Engine resources. The switch applies a preference algorithm when you enable Type 5 routes. For any destinations for which the switch has no Type 5 route, the switch uses Type 2 routes by default. Otherwise, the switch gives preference to:

- Type 2 routes for local ESI interfaces (locally learned routes)
- Type 5 routes for all other destinations within the data center or across data centers

You can refine these preferences by configuring routing policies in the EVPN routing instance to control the Type 5 routes that the switch imports and exports.

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

- **Optimized inter-subnet multicast support with symmetric bridge domain configuration in an EVPN-VXLAN fabric (QFX5110, QFX5120, QFX10002-36Q, and QFX10002-72Q)**—Starting in Junos OS Release 21.2R1, you can configure optimized inter-subnet multicast (OISM) on leaf devices and border leaf devices in an EVPN-VXLAN edge-routed bridging overlay fabric. This feature helps optimize the routing of multicast traffic across VLANs in an EVPN tenant domain. This feature uses a supplemental bridge domain (SBD) and a multicast VLAN (MVLAN) to route multicast traffic from or to devices outside of the fabric. This feature also works with existing IGMP snooping and selective multicast (SMET) forwarding optimizations to minimize replication in the EVPN core when bridging within tenant VLANs.

With this implementation, you must enable OISM and IGMP snooping on all the leaf and border leaf devices in the EVPN-VXLAN fabric. You also must configure the SBD and all tenant VLANs symmetrically on all leaf and border leaf devices in the fabric.

You can use OISM with:

- EVPN on the default-switch instance with VLAN-aware bundle service model (Layer 2)
- Routing instances of type vrf (Layer 3)
- EVPN single-homing or multihoming (all-active mode)
- IGMPv2
- Multicast sources and receivers within the EVPN data center
- Multicast sources and receivers outside the EVPN data center that are reachable through the border leaf devices

[See [Optimized Inter-Subnet Multicast in EVPN Networks.](#)]

- **Overlapping VLAN support for edge-routed bridging in an EVPN-VXLAN fabric (QFX5110 and QFX5120)**—Starting in Junos OS Release 21.2R1, you can map the host VLAN to the VLAN that is provisioned on the leaf device by using VLAN translation. The host VLAN is translated to the VLAN that is already configured on the leaf device before the packet is processed. Conversely, the packet egresses from the access port with the translated VLAN.

[See [vlan-rewrite](#).]

Forwarding Options

- **Remote port mirroring with VXLAN encapsulation (EX4650, QFX5120-32C, QFX5120-48T, and QFX5120-48Y switches)**—Starting in Junos OS Release 21.2R1, you can configure remote port mirroring in an EVPN-VXLAN environment. Remote port mirroring sends copies of packets to an output destination for remote monitoring. This feature supports VXLAN encapsulation of the mirrored packets so they can be sent to an output destination in a separate virtual network identifier (VNI) domain.

High Availability

- **Hardware-assisted inline BFD (QFX5120-32C and QFX5120-48Y)**—Starting in Junos OS Release 21.2R1, we support a hardware implementation of the inline BFD protocol in firmware form. The ASIC firmware handles most of the BFD protocol processing. The firmware uses existing paths to forward any BFD events that must be processed by protocol processes. The ASIC firmware processes the packets more quickly than the software, so hardware-assisted inline BFD sessions can have keepalive intervals of less than a second. These platforms support this feature for single-hop and multihop IPv4 and IPv6 BFD sessions.

[See [ppm](#) and [Bidirectional Forwarding Detection \(BFD\)](#).]

Interfaces

- **Flexible Ethernet support (QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.2R1, you can configure flexible Ethernet services to support a Layer 2 bridging interface while simultaneously supporting other encapsulation options on the same physical interface. You can configure a physical or aggregate Ethernet interface to simultaneously support Layer 2 bridging, Layer 3 IP routing, and VLAN-based CCC connections.

NOTE: On QFX10000 line of Switches running Junos OS releases earlier than Release 21.2R1, we do not support configuring `vlan-bridge` and any other encapsulations on an interface that has `flexible-ethernet-services` enabled.

[See [Flexible Ethernet Services Encapsulation](#).]

Juniper Extension Toolkit (JET)

- **BGP route service API supports programming routes with IP-IP encapsulation attributes (MX240, MX480, MX960, PTX1000, QFX5110, QFX5200, QFX10002, and QFX10008)**—Starting in Junos OS Release 21.2R1, you can use the BGP route service API to program BGP routes with IP over IP (IP-IP) encapsulation attributes. You can specify the tunnel type, the remote endpoint address, and the color of the route. Keep the following in mind:
 - The egress endpoint must be a unicast IPv4 address.
 - The colors encoded in `tunnel_encap` and `extended_community` must match.
 - If the encapsulation `ext_com` and the tunnel attribute are both present, the egress endpoint must match the next-hop address.

To enable this feature, configure the `bgp-signal` option at the `[edit routing-options dynamic-tunnels tunnel-name]` hierarchy level. The rest of your dynamic tunnel CLI configuration does affect the functionality of the programmed tunnels.

[See [dynamic-tunnels](#) and [JET APIs on Juniper EngNet.](#)]

Junos Telemetry Interface

NOTE: For Routing Engine telemetry sensors supported by this platform, see [Telemetry Sensor Explorer](#). If any Platform Forwarding Engine sensors have been added for this release, they are listed below

- **End-of-message notification for Routing Engine sensors (EX2300, EX4300, EX4300-MP, EX9200, MX240, MX960, MX10016, MX2010, MX2020, PTX1000, PTX3000, PTX10001, QFX5100, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we've introduced an end-of-message (EoM) Boolean flag for all Junos telemetry interface (JTI) Routing Engine sensors. The flag notifies the collector that the current wrap has completed for a particular sensor path. A wrap is a complete key-value data dump for all the leaves under a sensor path.

The EoM flag also enables the collector to detect when the end of wrap occurs without having to compare stream creation timestamp values that the collector receives from the packets. Comparing timestamp values is costly time-wise and delays data aggregation.

To use this feature with gRPC Network Management Interface (gNMI) transport or Remote Procedure Call (gRPC), retrieve the protobuf files from the relevant branch on the [Juniper Networks](#) download site:

- `GnmiJuniperTelemetryHeaderExtension.proto` (gNMI)

- agent.proto (for gRPC)

For example: <https://github.com/Juniper/telemetry/blob/master/20.3/20.3R1/protos/GnmiJuniperTelemetryHeaderExtension.proto>.

After you download and install the new protobuf files on a collector, the EoM field is present in the packets received.

[See [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **Monitoring and optimizing Packet Forwarding Engine sensor data export (PTX Series and QFX Series)**
—Starting in Junos OS Release 21.2R1, you can optimize Packet Forwarding Engine sensor data to dynamically determine how to export data as quickly as possible based on three sensor categories: heavy data (dynamic scale), medium data (predicted scale), and low data (fixed scale). In addition, you can use our new sensor to retrieve export details of all Packet Forwarding Engine sensors. Use the resource path `/junos/system/linecard/export/monitor` to monitor export details for each subscribed Packet Forwarding Engine sensor including:
 - Number of reaps
 - Number of wraps (a complete data set)
 - Number of packets sent
 - Average number of reaps and wraps
 - Timestamps for reaps and wraps

[See [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#) and [Guidelines for gRPC and gNMI Sensors \(Junos Telemetry Interface\)](#).]

- **Enable VOQ utilization monitoring with JTI (PTX1000, PTX5000, PTX10000, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.2R1, you can enable the export utilization data for CoS virtual output queues (VOQs) on aggregated Ethernet or physical Ethernet WAN interfaces. Using this feature, you can export peak buffer utilization data for a given queue with Junos telemetry interface (JTI). Monitoring this data can assist in preventing micro-bursts and high buffer utilization for a given queue because peak buffer utilization is transient and might not be reported by instantaneous queue depth.

To enable monitoring, include `queue-monitoring enable` at one of the following hierarchies:

- [edit class-of-service interfaces *if-name*]
- [edit class-of-service traffic-control-profiles *tcp-name*]
- [edit class-of-service schedulers *scheduler-name*]

To export data to a collector, include the resource path `/junos/system/linecard/qmon-sw` in a subscription.

[See [queue-monitoring](#), [show class-of-service interface](#), [show class-of-service traffic-control-profile](#), [show class-of-service scheduler-map](#) and [show interfaces voq](#) *interface-name*.]

Licensing

- **Juniper Agile Licensing (QFX5110-48S, QFX5110-32Q, QFX5120-32C, QFX5120-48T, and QFX5210-64C)**—Starting in Junos OS Release Evolved 21.2R1, the QFX switches support Juniper Agile Licensing.

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

Juniper Agile Licensing supports soft enforcement of software feature licenses. With soft enforcement, if you configure a feature without a license, Junos OS displays a warning when you commit the configuration except for PTP feature. However, the feature is operational. In addition, Junos OS generated periodic alarms indicating that you need the license to use the feature. You can see the list of alarms at [System Log Explorer](#).

[Table 13 on page 282](#) describes the licensing support with use case examples for QFX5110-48S, QFX5110-32Q, QFX5120-32C, QFX5120-48T, and QFX5210-64C.

Table 13: Supported Features on QFX5110-48S, QFX5110-32Q, QFX5120-32C, QFX5120-48T, and QFX5210-64C

QFX Switch License Model	Use Case Examples or Solutions	Detailed Features
Standard	Basic Layer 2 switching or basic Layer 3 forwarding	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	Data center fabric	<p>Advanced 1: BGP, FBF, GRE, IGMP version 1, IGMP version 2, and IGMP version 3, IS-IS, JTI, MC-LAG, Multicast Listener Discovery (MLD) version 1, MLD version 2, OSPF, RIP, VRF and VRRP</p> <p>Advanced 2: Advanced 1 features, CFM, ESI-LAG, EVPN-VXLAN, Layer 3 multicast, OAM, PTP, Q-in-Q, and Virtual Chassis</p>

Table 13: Supported Features on QFX5110-48S, QFX5110-32Q, QFX5120-32C, QFX5120-48T, and QFX5210-64C (Continued)

QFX Switch License Model	Use Case Examples or Solutions	Detailed Features
Premium	Data center interconnect or data center edge	Advance Enterprise Features, EVPN-MPLS, Layer 2 circuit, Layer 3 VPN (MPLS), LDP, RSVP, Segment routing, and SR-TE

In addition, you can install additional port bandwidth usage license to increase the port bandwidth usage.

[See [Flex Software License for QFX Switches](#), [Juniper Agile Licensing Guide](#), and [Configuring Licenses in Junos OS](#).]

Network Management and Monitoring

- **sFlow support for IP-IP traffic with VRF (PTX1000, PTX10002, PTX10008, QFX10002, and QFX10008)**—Starting in Junos OS Release 21.2R1, you can use sFlow technology to sample IP over IP (IP-IP) traffic that is hosted on multiple virtual routing and forwarding (VRF) instances. sFlow sampling now reports the extended router data correctly when the incoming and outgoing interfaces of the traffic reside on two different VRFs in IP-IP traffic for egress sampling.

[See [Overview of sFlow Technology](#).]

- **Support for syslog over TLS (EX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, you can transport syslog (control plane) over Transport Layer Security (TLS) protocol. Encapsulating syslog over 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
- 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.

Routing Options

- **Enhancements to prefix-limit and accepted-prefix-limit configuration statements, and updates to show bgp neighbor command (ACX1000, EX9200, MX Series, PTX5000, and QFX10002)**— Starting from Junos OS Release 21.2R1, the `prefix-limit` and `accepted-prefix-limit` configuration statements include the following options:
 - `drop-excess <percentage>`—If you include the `drop-excess <percentage>` option, the excess routes are dropped when the maximum number of prefixes is reached. If you specify a percentage, the routes are logged when the number of prefixes exceeds that percentage value of the maximum number.
 - `hide-excess <percentage>`—If you include the `hide-excess <percentage>` option, the excess routes are hidden when the maximum number of prefixes is reached. If you specify a percentage, the routes are logged when the number of prefixes exceeds that percentage value of the maximum number.

The `show bgp neighbor` command has been enhanced to display the following additional information:

- Count of prefixes that are dropped or hidden based on network layer reachability information (NLRI) when the maximum allowed prefixes threshold is exceeded.
- Alerts when a peer starts to drop or hide routes.
- Configuration details of the `prefix-limit` and `accepted-prefix-limit` configuration statements.

[See [prefix-limit](#), [accepted-prefix-limit](#), [show bgp neighbor](#), and [Multiprotocol BGP](#).]

Routing Protocols

- **Basic MVPN support with BGP sharding (cRPD, JRR200, MX2020, PTX5000, and QFX10002)**— Starting in Junos OS 21.2R1, we support the basic multicast virtual private network (MVPN) functionalities with BGP sharding.

NOTE: Sharding is not supported for the MVPN address family.

Services Applications

- **Support for MPLS, MPLS-IPv4, and MPLS-IPv6 inline active flow monitoring (QFX10002-60C)**— Starting in Junos OS Release 21.2R1, you can perform inline active flow monitoring for MPLS, MPLS-IPv4, MPLS-IPv6, and MPLS-over-UDP traffic. For MPLS-over-UDP flows, inline active flow monitoring allows you to look past the tunnel header to sample and report on the inner payload, at both the transit and egress nodes of the tunnel. We support IPFIX and version 9 templates but only ingress sampling.

[See [Inline Active Flow Monitoring of MPLS-over-UDP Flows.](#)]

Software Installation and Upgrade

- **Dynamic port speed detection for ZTP (QFX10002)**—Starting in Junos OS Release 21.2R1, you can use either WAN interfaces or management interfaces to automatically download and install the appropriate software and the configuration file on your device during the bootstrap process. Zero-touch provisioning (ZTP) automatically configures WAN interfaces based on the optics type, and then connects your device to the DHCP server to perform the bootstrap process.

[See [Zero Touch Provisioning.](#)]

System Management

- **Support for PTP SMPTE media profile (QFX5120-48T)**—Starting in Junos OS Release 21.2R1, you can enable the Society of Motion Picture and Television Engineers (SMPTE) profile to support video applications to enable capture, video edit, and playback to be used in professional broadcast environments. The standard allows multiple video sources to stay in synchronization across various equipment by enabling time and frequency synchronization to all devices.

[See [Understanding the PTP Media Profiles](#) and [Configuring the PTP Media Profiles.](#)]

- **Support for PTP boundary clock and enterprise profile (QFX5120-48T)**—Starting in Junos OS Release 21.2R1, you can enable the boundary clock and enterprise profiles, which are based on Precision Time Protocol (PTP) version 2 (PTPv2). The PTP enterprise profile enables the enterprise and financial markets to add a timestamp to the operations of different systems, and to handle a range of latencies and delays. The boundary clock has multiple network connections and can act as a source (primary) and a destination (client) for synchronization messages. It synchronizes itself to a best primary clock through a client port and supports synchronization of remote clock clients to it on primary ports.

[See [Understanding the Precision Time Protocol Enterprise Profile](#) and [IEEE 1588v2 PTP Boundary Clock Overview.](#)]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 286](#)

- [What's Changed in Release 21.2R2 | 287](#)
- [What's Changed in Release 21.2R1 | 287](#)

Learn about what changed in the Junos OS main and maintenance releases for QFX Series Switches.

What's Changed in Release 21.2R3

IN THIS SECTION

- [Network Management and Monitoring | 286](#)

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.](#)]

- **Changes to the NETCONF `<edit-config>` RPC response (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<edit-config>` operation returns an error, the NETCONF server does not emit a `<load-error-count>` element in the RPC response. In earlier releases, the `<edit-config>` RPC response includes the `<load-error-count>` element when the operation fails.

What's Changed in Release 21.2R2

IN THIS SECTION

- [Class of Service \(CoS\) | 287](#)
- [EVPN | 287](#)

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

- **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.

What's Changed in Release 21.2R1

IN THIS SECTION

- [Class of Service \(CoS\) | 287](#)
- [EVPN | 288](#)
- [Junos XML API and Scripting | 288](#)
- [Platform and Infrastructure | 288](#)
- [Layer 2 Ethernet Services | 289](#)
- [Network Management and Monitoring | 289](#)

Class of Service (CoS)

- **[edit class-of-service traffic-control-profiles] should be ordered-by system as per customers**—Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

- Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

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.

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.](#)]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See [request system scripts refresh-from](#) and [cert-file \(Scripts\)](#).]

Platform and Infrastructure

- **SSH session connection limit and rate limit per connection (PTX Series and QFX Series)**—We have introduced SSH `<connection-limit>` and `<rate-limit>` options at the `<edit system services ssh>` hierarchy levels to enable SSH connection limit and rate limit per connection. The default connection limit value is 75 connections and there is no default value associated with rate limit.

- **Support only for manual channelization on QSFP-100G-SR4-T2 optics (QFX5120-48T and QFX5120-32C)**—We recommend that you use the active optical cable (AOC) for auto-channelization. The QSFP-100G-SR4-T2 cables do not support auto-channelization. To use the QSFP-100G-SR4-T2 optics with an external breakout cable, you must configure the channelization manually by running the <channel-speed> statement at the edit chassis fpc slot-number pic pic-number (port port-number | port-range port-range-low port-range-high) hierarchy level.
- **Juniper Agile Licensing (QFX5120-48Y, QFX5110-32Q, and QFX5110-48S)**—Starting from this release onwards, the QFX 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 Guide](#).]

Layer 2 Ethernet Services

- **Link selection support for DHCP (QFX Series)**—We've introduced 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. Earlier to this release, the DHCP relay drops packets during the renewal DHCP process as the DHCP Server uses the leaf's address as a destination to acknowledge DHCP renewal message.

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

Network Management and Monitoring

- **Chef and Puppet support removed (EX Series except EX4400, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, Junos OS products that were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS. FreeBSD 12.x based Junos OS does not support installing existing Chef or Puppet packages.
- **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](#).]

- **Changes to <commit> RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server's response for <commit> operations includes the following changes:
 - If a successful <commit> operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.
 - The NETCONF server response emits the <source-daemon> element as a child of the <error-info> element instead of the <rpc-error> element.
 - If you also configure the `flatten-commit-results` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server suppresses any <commit-results> XML subtree in the response and only emits an <ok/> or <rpc-error> element.

[See [Configuring RFC-Compliant NETCONF Sessions](#).]

Known Limitations

IN THIS SECTION

- [Platform and Infrastructure | 291](#)
- [Infrastructure | 292](#)
- [Routing Protocols | 292](#)

Learn about known limitations in Junos OS Release 21.2R3 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.

Platform and Infrastructure

- Junos OS might hang trying to acquire the SMP IPI lock while rebooting when it is running as a VM on Linux and QEMU hypervisor. [PR1385970](#)
- On the QFX10000 line of devices, if an analyzer is configured to mirror traffic of an input aggregated Ethernet interface and a new member is added to the same aggregated Ethernet interface, then the analyzer might not provide sample packets that flow through a newly added child interface. [PR1417694](#)
- This issue occurs due to PECHIP limitation when underlay is tagged. After de-encapsulation when inner packet is recirculated it still retains the VLAN tag property from the outer header since outer header was tagged. Thus 4 bytes of inner tag got overwritten in inner packet and packet got corrupted which will result in EGP chksum trap seen in PECHIP. Fixing PECHIP limitation in software has high risk. It will be accommodated in a future release. As a workaround, enable `encapsulate-inner-vlan` statement. [PR1435864](#)
- On QFX10002 switches in a dynamic IP-IP tunnel transit scenario, when sFlow egress sampling is enabled on an aggregated Ethernet interface in an ECMP case, the sFlow export data does not include the nextHop field. [PR1533307](#)
- On QFX5100 devices not running the qfx-5e codes (non-TVP architecture), when an image with the Broadcom SDK upgrade (6.5.x) is installed, the CPU utilization might go up by around 5%. [PR1534234](#)
- On QFX5200 and QFX5100 switches with the IPIP tunnel feature, `show dynamic-tunnels database statistics` command output shows extra packet counts (that is, sampled packets when sFlow is enabled). [PR1555922](#)
- The `rpd` crash is observed when the device reboot and/or daemon restart. The Junos-Evolved based PTX products are impacted while Junos-Evolved based QFX and EX products are not impacted by this issue. [PR1567043](#)
- On QFX10002-72Q devices, configuration validation is not supported during an image downgrade or upgrade. [PR1579050](#)
- With multicast sampling enabled, some packets might be dropped when samples received from HW match the multicast replication rate configured. [PR1586690](#)
- On QFX5000/EX46xx, IRACL filters will not be able to match on VxLAN tunnel terminated packets. [PR1594319](#)

Infrastructure

- When upgrading from pre Junos Release 21.2 to Release 21.2 and onward, validation and upgrade will fail. The upgrading requires using of `no-validate` statement. [PR1568757](#)

Routing Protocols

- On QFX5120-48YM platform, when scale of IPv4 and IPv6 routes are present in LPM profile, few of the IPv6 routes will not be installed when the ports on which routes are learnt is flapped due to LPM table full error. [PR1557655](#)

Open Issues

IN THIS SECTION

- [EVPN | 293](#)
- [Infrastructure | 293](#)
- [Interfaces and Chassis | 293](#)
- [Layer 2 Ethernet Services | 294](#)
- [MPLS | 294](#)
- [Platform and Infrastructure | 294](#)
- [Routing Protocols | 299](#)

Learn about open issues Junos OS Release 21.2R3 for QFX Series switches.

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

EVPN

- End-hosts might not communicate via Ethernet VPN with Virtual Extensible LAN encapsulation (EVPN-VxLAN) domain after Ethernet Segment Identifier (ESI) failover. This issue affects QFX5000 platforms only. Please refer to restoration steps when this issue is encountered. [PR1584595](#)
- Modifying the I-ESI value is a traffic effecting event. If this must be done, then use the following steps to avoid this issue.

1. Deactivate interconnect stanza for the routing-instance in question.
2. Modify the I-ESI value.
3. Activate the interconnect stanza.

[PR1600600](#)

- This problem happens only with translation VNI when mac is moved one from DC1 to DC2. VM move across DC where there is no translate VNI configuration in the interconnect works as designed. [PR1610432](#)
- EVPN Local ESI Mac limit configuration might not become effective immediately when it has already learned remote MH Macs. Clear the Mac table from all MH PEs and configure the Mac limit over local ESI interfaces. [PR1619299](#)
- User cannot change I-ESI on multi-homing GW nodes at the same time. There will be some gap in commit in two different GW nodes. During the gap, there will be different I-ESI on MH GW nodes, which will cause the loop for a short duration. Due to the loop, mac goes to duplicate mac detection state. To clear this duplicate macs, user has to issue clear duplicate mac detection. As a workaround, deactivate interconnect on multi-homing GW nodes before changing the I-ESI, commit, and then change I-ESI and activate interconnect. [PR1624981](#)

Infrastructure

- The following messages are seen during FTP:ftpd[14105]: bl_init: connect failed for `/var/run/blacklistd.sock' (No such file or directory). [PR1315605](#)

Interfaces and Chassis

- In QFX, when BUM traffic is sent on MCLAG, Mac entries are learnt on ICL interface as DLR when ICL is flapped as mac learning. This may cause the traffic loss with certain traffic flow. [PR1639713](#)

Layer 2 Ethernet Services

- If request `system zeroize` does not trigger zero-touch provisioning, re-initiate the ZTP as a workaround. [PR1529246](#)
- The DHCP client configuration is coming from two places, that is, AIU script and vsdk sandbox. The DHCP client configuration coming from AIU script has the serial Id in vendor id where as the default configuration from sandbox doesn't have it. There is no impact on functionality or service. [PR1601504](#)

MPLS

- The `rsvp interface update threshold` configuration syntax has changed between Junos OS Release 18.2X75-D435 and Junos OS Release 20.3X75-D10 to include curly braces around the threshold value. Upgrading and downgrading between these releases is not entirely automatic. The user must delete this stanza if configured before the downgrade and then manually reconfigure. [PR1554744](#)

Platform and Infrastructure

- The `commit synchronize` command fails because the kernel socket gets stuck. [PR1027898](#)
- Arrival rates are not seen at system level when `global-disable fpc` is configured on QFX. [PR1438367](#)
- When the DHCP relay mode is configured as `no-snoop`, we are observing the offer gets dropped due to incorrect asic programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. [PR1530160](#)
- On a PTX Series router or QFX10000 switch with a third-generation FPC, an error message is displayed when the FPC goes online or offline. [PR1322491](#)
- QFX10000:Source MAC and TTL values are not updated for routed multicast packets in EVPN-VXLAN. [PR1346894](#)
- Backup Routing Engine might crash after GRES occurs continuously for more than 10 times. [PR1348806](#)
- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. [PR1362609](#)

- Due to transient hardware condition, single-bit error (SBE) events are corrected and have no operational impact. Reporting of those events had been disabled to prevent alarms and possibly unnecessary hardware replacements. This change applies to all platforms using Hybrid Memory Controller (HMC). [PR1384435](#)
- The unified ISSU is not supported on QFX5200 switches and fails from Junos OS Release 17.2X75-D43.2 to some target versions. Also, dcpfe crash might be seen. [PR1438690](#)
- There is a timing issue during the sxe interface bring up (w.r.t i40e driver). This can be recovered by rebooting the complete board. [PR1442249](#)
- In race condition, 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](#)
- The storm-control does not rate-limit ARP packets on QFX10000 although shutdown action works. [PR1461958](#)
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. [PR1462548](#)
- On QFX5000/EX4600 Series platforms with "instance-import", deleting route which has "next-table" used might result in unexpected route next-hop. [PR1477603](#)
- When running 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](#)
- On Junos PTX and 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](#)
- On a fully scaled system where all the slices are utilized by different families of CLI filters, if you try to call delete for one family and add/change for another family with a higher number of filter terms which requires either expansion of the filter or creation of a new filter, the Packet Forwarding Engine fails to add the new filter as we are getting messages out of sequence that is, the add/change of filter is called earlier than the delete of another filter that will free up the slices. [PR1512242](#)
- MSDP sessions might reset after a GRES reset even when nonstop routing state is synchronized and ready for switchover. [PR1526679](#)
- PR 1530951: FIPS mode is not supported on 20.4R1-EVO. [PR1530951](#)
- On QFX5100 devices not running the qfx-5e codes (non-TVP architecture), when an image with the Broadcom SDK upgrade (6.5.x) is installed, the CPU utilization might go up by around 5%. [PR1534234](#)

- On QFX5000 serial platform, under Ethernet VPN and Virtual Extensible LAN (EVPN-VXLAN) spine-and-leaf environment, packets sent via VXLAN tunnel might lose Virtual Tunnel End Point (VTEP) IP address (source IP address (SIP)). Packets without SIP could cause memory leak. This issue rarely happens because it is difficult to be reproduced. [PR1536895](#)
- "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](#)
- EVPN-VxLAN: vmcore files are seen on Master and backup Routing Engine of QFX10k8 with L2/L3 Multicast configuration. [PR1539259](#)
- Broadcom has updated that BCMX calls are deprecated and needs to be replaced with BCM calls. [PR1541159](#)
- 100G AOC from Innolight does not come up after multiple reboots. It recovers after interface enable/disable. [PR1548525](#)
- Users cannot subscribe to any path that ends with "key". [PR1553534](#)
- ISSU is not supported from releases below 20.4 to releases 20.4 and above. There is a major SDK upgrade from 6.3.2 to 6.5.16, due to which the Warm boot feature needed for ISSU is not supported by our vendor. [PR1554915](#)
- 5M DAC connected between QFX10002-60C and MX2010 doesn't link up. But with 1M and 3M DAC this interop 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](#)
- In Release 20.2, some features will show up as a licensed feature. Customer would see alarms, commit warnings and show system license output as below. However, there would be no functional impact. user@QFX5120> show system license License usage:Licenses Licenses Licenses ExpiryFeature name used installed neededesi-lag 1 0 1 invalid. [PR1558017](#)
- On QFX5120-48Y switches, amber LEDs are displayed for the fan modules after upgrading to Junos OS Release 20.2R1 and later. The LEDs are on continuously even if there is no fault in the fans. [PR1558407](#)
- To avoid the additional interface flap, interface hold time needs to be configured. [PR1562857](#)
- Starting in Junos OS Release 21.1R1, Junos 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, so far (that is, until 20.4R1), the python script had #!/usr/bin/python as the first line (ie 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](#)
- In mixed QFX5100, EX4300 VCF setup, duplicate traffic might be observed for some Layer 3 multicast traffic streams . [PR1568152](#)
- On QFX5000, in EVPN_VXLAN deployment, BUM traffic replication over VTEP might send out more packets than expected. [PR1570689](#)
- In EVPN/VXLAN scenario with OSPF configured over the IRB, OSPF sessions might not get established due to connectivity issues. [PR1577183](#)
- Observed the partial traffic loss after disabling the protected link on R2 hence seeing the convergence delay for link-protection for PE1_P link. [PR1579931](#)
- On QFX5100, while checking DHCP Smart Relay over IRB interfaces, the renew-ack's may not be seen in the dhcp client. [PR1581025](#)
- In a 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 development setup. [PR1581767](#)
- When physical loopback is used and both the ports are with EP style in the same RSPAN VLAN it can lead to flooding. [PR1581876](#)
- RPD core file is seen `@rt_iflnh_set_nhid` . Core file is due to assertion caused by failure of `hbt_insert` for `nhid` belonging to an `ifl`. It is seen that there is a duplicate entry present which causes the `hbt_insert` failure. [PR1588128](#)
- The 'input ingress' and 'input egress' together for the same port will not work in mirroring with VXLAN encapsulation. [PR1589854](#)
- On QFX/EX series switches with Broadcom chip as Packet Forwarding Engine (PFE), 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, greater than 1496 bytes) might be dropped and not sent to the IS-IS neighbors. The following is the product list of QFX/EX series switches with Broadcom chip as Packet Forwarding Engine. QFX5100/QFX5110/QFX5120/QFX5130/QFX5200/QFX5210/QFX5220 EX2300/EX3400/EX4300/EX4600/EX4650 [PR1595823](#)
- On the QFX10000 series platforms, the process `dcpfe/FPC` crash might be observed in boot time if rebooting the devices. [PR1597479](#)

- There is a remote possibility that during many reboots, the Junos VM goes into a state where NMI is needed to continue the reboot. There is no workaround for this and a subsequent reboot does not seem to hit this issue. [PR1601867](#)
- During reboot in certain instances device gets into a state where Junos virtual machine hangs until the NMI is triggered and reboots fully. [PR1602360](#)
- Chassisd generates "Cannot read hw.chassis.startup_time value: m" every 5 seconds on qfx10008. [PR1603588](#)
- On QFX5100, optical power is seen after detached and attached QSFP on disable interface. [PR1606003](#)
- In QFX10002-60C under mac statistics "output-mac-control-frames" and "output-mac-pause-frames" does not increment. [PR1610745](#)
- QFX10002/QFX10008/QFX10016: As per design change, devices have max token allocation limit of 104k combined for I2/I3/BUM routes. These tokens are used as egress nexthop IDs for route lookup in HW. Out of 104k tokens, 8k tokens are reserved for maximum VXLAN tunnels and 16k tokens are reserved for IRB interfaces, and locally learned ARP/NDP Nexthops also require tokens to install in HW which will be allocated from free pool of tokens left after the reservations. So, total tokens available tokens in free pool after reserving [8k(vxlan tunnels) + 16k(IRBs)] is 80k tokens. Thus, maximum of 80k local ARP entries can be supported on QFX10k (Elit/Ulimate) devices.
QFX10002-60c: As per current design, device have max token allocation limit of 96k combined for I2/I3/BUM routes. These tokens are used as egress nexthop IDs for route lookup in HW. Out of 96k tokens, 8k tokens are reserved for maximum VXLAN tunnels and 10k tokens are reserved for IRB interfaces, and locally learned ARP/NDP Nexthops also require tokens to install in HW which will be allocated from free pool of tokens left after the reservations. So, total tokens available tokens in free pool after reserving [8k(vxlan tunnels) + 10k(IRBs)] is 78k tokens. Thus, maximum of 80k local ARP entries can be supported on QFX10k (Elit/Ulimate) devices. [PR1616224](#)
- In "Remote Mirroring with VXLAN Encapsulation" Physical/Softloopback ports are used to achieve the VXLAN encapsulation of the mirrored traffic. When mirrored traffic packets are of NS/ARP these packets are sent to the CPU and are re-injected back to RSPAN VLAN, which will cause the LOOP between the loop-backed ports and in turn sent to the remote collector. [PR1631618](#)
- On QFX platforms, in Q-in-Q scenario when 'input-native-vlan-push' statement is disabled inner Virtual LAN (VLAN) might be stripped off if it matches the outer VLAN. Traffic drop might be observed in this scenario. [PR1631771](#)
- chassisd crashed after configuring chassis disk-partition. The cli command is not supported by QFX10008 and QFX10016 platforms. Hence disabling the same. [PR1635812](#)
- Child link is not coming up after loaded the lag configuration. [PR1646495](#)

Routing Protocols

- Multicast traffic is overusing the switch core when igmp-snooping is removed. The MCSNOOPD will generate core files due to the changes in mrouter interfaces and routes. [PR1569436](#)
- On QFX10002 platforms, the multi-hop BFD session might flap if collecting RSI or some other outputs (such as show interface or configuration). It is caused by the missing BFD packets because the PPMAN thread is not scheduled within the BFD timers which are 300 milliseconds with a multiplier of 3. [PR1589765](#)
- When the 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](#)
- On certain conditions where underlay session flapped due to interface down event, it may possible to see the flap in overlay bfd session due to delay in route install to reach the packet to the neighbor. [PR1618118](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.2R3 | 300](#)
- [Resolved Issues: 21.2R2 | 306](#)
- [Resolved Issues: 21.2R1 | 312](#)

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R3

IN THIS SECTION

- [Class of Service \(CoS\) | 300](#)
- [EVPN | 300](#)
- [General Routing | 301](#)
- [High Availability \(HA\) and Resiliency | 301](#)
- [Infrastructure | 301](#)
- [Layer 2 Ethernet Services | 301](#)
- [MPLS | 301](#)
- [Platform and Infrastructure | 301](#)
- [Routing Policy and Firewall Filters | 306](#)
- [Routing Protocols | 306](#)
- [User Interface and Configuration | 306](#)

Class of Service (CoS)

- Transit packets from local to remote VTEP might get punted to CPU and cause DDoS events. [PR1489233](#)
- The dcpfe core files might be seen in auto-channelization scenario or when SFP is plugged out. [PR1616847](#)
- The uplink interface remains down for a longer duration due to VXLAN scaled configuration. [PR1631448](#)

EVPN

- A few ARP/ND/MAC entries for Vlans are missing with MAC-VRF configuration. [PR1609322](#)
- IRB proxy-arp unrestricted might not work if EVPN/I2alm proxy is enabled. [PR1613201](#)
- Multiple memory leaks might be seen leading to process rpd crash. [PR1626416](#)
- The MAC address might not be visible in the EVPN/VXLAN environment. [PR1645591](#)

General Routing

- Memory usage continuously increase is observed on backup chassis if subscriber service is enabled. [PR1595238](#)

High Availability (HA) and Resiliency

- During unified ISSU package signature validation might fail and the upgrade might not happen. [PR1575680](#)
- Memory leaking might occur on backup Routing Engine when ksyncd is in inconsistent state and had encountered an initialization error. [PR1601960](#)

Infrastructure

- The alarm "Host 0 Active Disk Usage Exceeded" might be generated due to a large number of files under `/var/log/journal` which were held by the Eventd daemon. [PR1601251](#)

Layer 2 Ethernet Services

- Enabling DHCP on Junos and Junos Evo 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](#)
- Traffic loss seen on the QFX5000 line of switches after STP topology change. [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 may affect communication on IPv6 link-local addresses. [PR1600085](#)
- The packet drop might be seen on FPC on Trio based platforms. [PR1631313](#)
- On the QFX5110 line of switches, the untagged traffic routed over native-vlan might be dropped. [PR1560038](#)
- Multiple entries to vlan-id-list might not work in an EVPN-VXLAN scenario. [PR1564403](#)
- The na-grpcd process might crash during longevity tests. [PR1565255](#)

- MAC addresses might not be relearned successfully after MAC address age timeout. [PR1567723](#)
- QFX10K2-60C: Disk missing alarms are not seen. [PR1573139](#)
- When soft loopback port and analyzer configurations are committed together, Mirror ingress to local port is not working . [PR1581542](#)
- QFX5000 series - show route detail might not show Next-hop type IPoIP Chained comp nh in the output (Display only - no operation impact) [PR1584322](#)
- The QFX5000/10000 device might get hanged after reboot for sometime. [PR1584902](#)
- High FPC CPU utilization might be seen on PTX10002-60C/QFX10002-60C platform. [PR1585728](#)
- The syslog ERROR message might be seen when deactivating Bridge domains/VLANs. [PR1589138](#)
- QFX5210-64C - PSU jfirmware upgrade through Junos. [PR1589572](#)
- The DCI InterVNI and IntraVNI traffic might be dropped silently in gateway node due to the tagged underlay interfaces. [PR1596462](#)
- The l2alm fails to send IPC message to the l2ald which might cause the FPC to crash. [PR1596615](#)
- Error message error: syntax error: request-package-validate will be seen on device CLI output during non stop software upgrade. [PR1596955](#)
- The interface on SFP-T or SFP-SX might stop forwarding traffic on EX4600. [PR1598805](#)
- EVPN-VXLAN:QFX10008: RE1 went to DB prompt when tried loading profile configurations over LRM configurations. [PR1598814](#)
- The SFP-T port might stop forwarding traffic on EX4600 platforms. [PR1600291](#)
- The VCP might not form adjacency after rebooting the master FPC in Virtual Chassis scenario. [PR1600398](#)
- QFX5200: Observed dcpfe core files while testing unified ISSU from Junos OS Release 21.1R1.11 to Release 21.2R1.7. [PR1600807](#)
- Removing and adding Virtual Chassis ports might cause the FPC to reboot. [PR1601557](#)
- InterDC traffic loss might be seen in MAC-VRF EVI with trap stats "dlu.unicode.discard ." [PR1601961](#)
- EVPN/VXLAN arp-suppression does not respond to ARP request when VLAN ID under interface (IFL) is different with VLAN ID under vlan (BD) in SP style. [PR1602318](#)
- On QFX5120s, even after deactivating analyzer configuration, traffic is getting mirrored. [PR1603192](#)

- Unicast DHCP packets might get flooded when DHCP relay is configured in non-default routing-instance. [PR1603444](#)
- The carrier transition counter might not get incremented upon link flap after the reboot. [PR1605037](#)
- On QFX5110 Virtual Chassis (VC) setup, removing and adding of VC ports might cause the VC ports to remain in down state sporadically. [PR1606705](#)
- FPC might crash post firewall filter configuration changes in QFX platforms. [PR1608610](#)
- An additional VLAN tag might be added for Point-to-Point Protocol over Ethernet (PPPoE) packets on QFX10016. [PR1610012](#)
- Continuous Layer 3 traffic drop might be observed with MC-LAG configuration on QFX10000 platforms. [PR1610173](#)
- MAC move or MAC flap might be triggered in the QFX5000 Virtual Chassis environment. [PR1610295](#)
- Inter-vlan connectivity might be lost in an EVPN-VXLAN with CRB topology. [PR1611488](#)
- Continuous FPC crash and dcpfe core files might be seen on QFX10002-60C and PTX10002-60c platforms. [PR1612871](#)
- ARP resolution for data traffic received over Type5 might fail. [PR1612905](#)
- Removing the optical module "JNP-SFPP-10GE-T" from a port might cause certain ports to go down. [PR1614139](#)
- On QFX5000 VLAN firewall filter is not deleted in Packet Forwarding Engine after configuration change. [PR1614767](#)
- The l2ald process might crash in EVPN scenario. [PR1615269](#)
- Slow memory leak (32 bytes each time) of rpd might be seen. [PR1616065](#)
- The BFD session might flap on the QFX5120-48YM platform. [PR1616692](#)
- The l2cpd core file is seen with FIP snooping configuration on any interface. [PR1617632](#)
- BGP routes learnt through type 5 EVPN routes might not get activated. [PR1617878](#)
- BFD session might get stuck in init state after l2-learning restart due to incomplete ARP resolutions. [PR1618280](#)
- Core files might be seen on EX and QFX devices after configuration changes. [PR1618352](#)
- Traffic might be dropped when IRB is configured and removed from VLAN. [PR1618425](#)

- Dot1x based firewall policers are not supported. [PR1619405](#)
- The process dcpfe might crash after performing VXLAN VNI configuration change and delete on QFX5000 and EX series platforms. [PR1619445](#)
- Disabled VCP (Virtual chassis port) will be UP after the optic on it 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](#)
- QFX-5120: Observing error "tvp_is_qsfp_has_single_led ioctl call failed ret:-1" 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](#)
- Interface on QFX52xx not coming up after swapping from 100G to 40G. [PR1623283](#)
- MACsec session might flap if multiple logical interfaces are created on single physical interface. [PR1624524](#)
- In rare circumstances, PKID might crash and generate a core file when there was limited memory available on the Routing Engine. [PR1624613](#)
- 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 statement no-incoming-port is not applied after reboot on QFX10002/QFX10008 platforms. [PR1625988](#)
- The third 802.1Q tag might not be pushed onto the stack in the Q-in-Q tunneling. [PR1626011](#)
- 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](#)

- Layer 3 traffic failure might be observed with scaled MC-LAG configuration on QFX10002/QFX10008/QFX10016 platforms. [PR1627846](#)
- 802.1p BA classification might not work on mixed Virtual Chassis when interface has a DSCP and 802.1p classifier. [PR1628447](#)
- DHCP inform ack might be sent with broadcast address when DHCP smart relay is used. [PR1628837](#)
- The vmhost crash might be seen in a rare condition when route addition and change. [PR1629200](#)
- Some ports (port 20 and above) on QFX5110-32Q Virtual Chassis might not come up after a device restart or Packet Forwarding Engine reboot. [PR1629231](#)
- Traffic might get dropped when family ethernet-switching is configured on the interface in Q-in-Q scenario. [PR1629680](#)
- The "show interface extensive" command might not show Local/Remote fault.
- LACP timeout might be observed during high CPU utilization. [PR1630201](#)
- 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 AE interfaces on QFX5K/EX4600/EX4650 platforms. [PR1633452](#)
- Traffic loss is observed after MAC ages. [PR1633879](#)
- The VCPs connected with the AOC cable might not come up after upgrading to Junos OS Release 17.3 or later releases. [PR1633998](#)
- Data might not be exchanged via EVPN-VxLAN domain. [PR1635347](#)
- Silent drop in traffic 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/transceiver replacement. [PR1638045](#)
- Targeted broadcast or WOL feature may not work on QFX 5000 platforms. [PR1638619](#)
- MAC-move might be observed when dhcp-security is configured. [PR1639926](#)
- The KRT queue might get stuck with the error- 'ENOMEM -- Cannot allocate memory'. [PR1642172](#)
- ICMP TTL exceeded packets are not sent out of the switch. [PR1643457](#)

- Packets are dropped in ingress QFX5000 with EVPN-LAG multihoming due to VP-LAG programming issue. [PR1644152](#)

Routing Policy and Firewall Filters

- 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 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](#)
- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific BGP export policies. [PR1626367](#)
- The BFD session might be down when multiple addresses of same subnet are configured. [PR1635700](#)

User Interface and Configuration

- The core files may not get deleted using CLI "file delete /var/core/*/vmcore*". [PR1624562](#)

Resolved Issues: 21.2R2

IN THIS SECTION

- [Class of Service \(CoS\) | 307](#)
- [EVPN | 307](#)
- [General Routing | 307](#)
- [Interfaces and Chassis | 307](#)
- [Layer 2 Ethernet Services | 307](#)
- [Platform and Infrastructure | 308](#)

- Routing Protocols | 311
- User Interface and Configuration | 311

Class of Service (CoS)

- The TCP-ECN traffic might not be forwarded with high priority. [PR1585854](#)

EVPN

- Configuring the `static-mac` and `no-mac-learning` simultaneously on the VXLAN interface causes stale MAC and IP entry in the EVPN database. [PR1576147](#)
- Traffic loss might be seen under an EVPN-VXLAN scenario when MAC-IP moves from one CE interface to another. [PR1591264](#)
- The device announces `router-mac`, `target`, and EVPN-VXLAN community to BGP IPv4 NLRI. [PR1600653](#)
- Traffic sent by the QFX5000 leaf to remote leaf with link down. [PR1605375](#)
- In an EVPN-VXLAN scenario, a few ARP ND MAC entries for EP style VLANs are missing with MAC-VRF configuration. [PR1609322](#)

General Routing

- Memory usage increases continuously on backup chassis if the subscriber service is enabled. [PR1595238](#)

Interfaces and Chassis

- Removing the configuration from an interface stanza might cause the `dcpfe` process to crash. [PR1594356](#)

Layer 2 Ethernet Services

- The DHCP client might go offline for about 120 seconds after sending the DHCPINFORM message. [PR1587982](#)

Platform and Infrastructure

- The interface might not come up with 1 Gigabit optics. [PR1554098](#)
- The interface might go into blocking state impacting the traffic when the link-protection switches from primary to backup. [PR1555294](#)
- On QFX5100 platforms, the Virtual Chassis Port (VCP) might not come up after upgrading. [PR1555741](#)
- Upon receipt of specific sequences of genuine packets destined to the device, the kernel crashes and restarts. [PR1557881](#)
- On 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 ARP resolution might fail causing traffic issues. [PR1561588](#)
- The na-grpcd process might generate core files during longevity tests. [PR1565255](#)
- On QFX10000 Series platforms, DCPFE/FPC might crash if the ARP MAC move happens. [PR1572876](#)
- On QFX10K2-60C switches, disk missing alarms are not seen. [PR1573139](#)
- On QFX Series switches, 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 port might not bring down immediately during some abnormal type of line card reboot on the QFX10000 platforms. [PR1577315](#)
- On QFX5100 switches, some 40G ports might not be channelized successfully. [PR1582105](#)
- On QFX5000 platforms, firewall filter is not getting programmed after deleting a large filter and adding a new one in a single commit. [PR1583440](#)
- The QFX5000 and QFX10000 line of switches might hang for sometime after rebooting. [PR1584902](#)
- The zero touch provisioning (ZTP) process might silently drop or discard the traffic. [PR1585057](#)
- The na-grpc process crash might be seen and existing telemetry connections will be disconnected. [PR1587956](#)
- In an EVPN-VXLAN scenario, 50 percent traffic loss might be observed. [PR1589547](#)
- On QFX5210-64C switches, PSU firmware upgrades through Junos OS. [PR1589572](#)

- The MPLS traffic might not be forwarded after the aggregate interface flap on the QFX5120 switches. [PR1589840](#)
- VXLAN DDoS violation might occur when disabling the port mirror analyzer output interface. [PR1590150](#)
- Virtual Chassis mastership is changed and connection is dropped after renumbering the backup member ID. [PR1590358](#)
- On the QFX5120-48T switches, after removing 1G speed on interfaces, it does not come back as 10G. [PR1591038](#)
- The xSTP might not get configured when enabled on an interface with SP style configuration. [PR1592264](#)
- Routing Engine kernel might crash due to logical interface of aggregated interface adding failure in Junos kernel. [PR1592456](#)
- The IPv4 fragmented packets might be broken if the PTP transparent clock is configured. [PR1592463](#)
- On QFX10002, QFX10008, QFX10016 switches, MPLS traffic might get discarded on passive monitoring interface. [PR1592693](#)
- Multiple crashes with toe_interrupt_errors might be observed. [PR1593025](#)
- BFD session might flap during Routing Engine switchover. [PR1593244](#)
- The dcpfe process might crash in an EVPN-VXLAN scenario. [PR1593950](#)
- Packet drop might occur in 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 configuring a static ECMP route with the same number of next hops as the existing ECMP route. [PR1594573](#)
- The label field for the EVPN Type 1 route is set to 1. [PR1594981](#)
- The re-installation of the Type-5 tunnels might fail in an EVPN-VXLAN scenario. [PR1595197](#)
- The DCI InterVNI and IntraVNI traffic might get silently dropped and discarded in a gateway node due to the tagged underlay interfaces. [PR1596462](#)
- The mscsnoopd process might crash during deleting or adding Layer 2 forwarding configuration after performing a unified ISSU. [PR1596483](#)
- The fpc0 bcm pkt reinsert failed logs were written in the log messages in an aggressive way. [PR1596643](#)

- 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 the MACsec configuration on a logical interface does not take effect. [PR1597848](#)
- Socket connection drops due to keepalive timer expiration with port 33015. [PR1598019](#)
- On QFX5000 line of switches, sFlow sample rate setting causes IRB to not respond to ICMP traffic. [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](#)
- On QFX10002-60C switches with IRB interface, the Layer 3 traffic might be dropped or discarded silently. [PR1599692](#)
- Unable to disable the management port em1. [PR1600905](#)
- On QFX5120-48Y switches, dc-pfe core files are generated while issuing the show pfe vxlan nh-usage in an ERB EMC scenario with 6000 ARP entries. [PR1601949](#)
- The IPv6 traffic might be impacted when an IPv6 route resolves over a dynamic tunnel. [PR1602007](#)
- The egress interface of the GRE tunnel is not updated dynamically when the destination to the tunnel changes. [PR1602391](#)
- The FPC goes down and dcpfe core files are generated in some cases. [PR1602583](#)
- Traffic loss might be seen in a MC-LAG scenario on QFX platforms. [PR1602811](#)
- Traffic drop might be observed on the QFX5000 line of platforms in a Virtual Chassis scenario where the firewall filter is configured. [PR1602914](#)
- On an EVPN-VXLAN enabled endpoint, dot1x authentication might not work. [PR1603015](#)
- On QFX5120S switches, traffic gets mirrored even after deactivating analyzer configuration. [PR1603192](#)
- Packet loss might be seen on the filter-based GRE deployments. [PR1603453](#)
- Duplicate packets might be seen when you bring up all the interfaces on the spine switches. [PR1604393](#)
- On QFX5210-64C switches, the carrier transition counter does not increment on link flap after rebooting. [PR1605037](#)

- MAC move might be seen between the ICL and MC-LAG interface if you add or remove VLANs on the ICL interface. [PR1605234](#)
- Multicast streams might stop flooding in a VXLAN setup. [PR1606256](#)
- Virtual Chassis ports might remain in down state after removing and adding. [PR1606705](#)
- The LLDP packets received on a VXLAN enabled port might be flooded unexpectedly. [PR1607249](#)
- On QFX Series switches, the fxpc process might crash and generates a core file. [PR1607372](#)
- Ping to loopback and IRB interfaces over Type 5 fails. [PR1610093](#)
- Continuous Layer 3 traffic drop is observed with MC-LAG configuration on QFX Series platforms. [PR1610173](#)
- Agile licensing might vanish after Virtual Chassis mastership switchover or reboot. [PR1610272](#)
- MAC move or MAC flap might be triggered on the QFX5000 Virtual Chassis environment. [PR1610295](#)
- On QFX10002-60C and PTX10002-60C switches, FPC crashes continuously and generates dcpfe core file. [PR1612871](#)
- On QFX5000 line of switches, the VLAN firewall filter is not deleted in the Packet Forwarding Engine after configuration change. [PR1614767](#)
- The l2ald process crashes and generates core files in an EVPN scenario. [PR1615269](#)
- The BFD session might get stuck in the init state after Layer 2 learning restarts due to incomplete ARP resolutions. [PR1618280](#)

Routing Protocols

- The remaining BFD sessions of the aggregated Ethernet interface flap continuously if one of the BFD sessions is deleted. [PR1516556](#)
- Traffic loss might be seen when the IPv6 traffic forwarded by the IPv4 GRE tunnel. [PR1582408](#)
- The BGP egress TE routes lose to BGP routes using the same protocol preference. [PR1593332](#)
- IPv4 static route might still forward traffic unexpectedly even when the static route configuration is deleted. [PR1599084](#)

User Interface and Configuration

- The system archival might not work inside a routing instance. [PR1572228](#)

Resolved Issues: 21.2R1

IN THIS SECTION

- [Class of Service \(CoS\) | 312](#)
- [EVPN | 312](#)
- [Forwarding and Sampling | 312](#)
- [Interfaces and Chassis | 312](#)
- [Layer 2 Features | 313](#)
- [Layer 2 Ethernet Services | 313](#)
- [Platform and Infrastructure | 313](#)
- [Routing Protocols | 316](#)
- [User Interface and Configuration | 320](#)

Class of Service (CoS)

- Dscp classifier doesn't work and all packets are sent to single queue. [PR1585361](#)

EVPN

- On the QFX10000 devices, the l2ald process generates the core file at l2ald_VXLAN_ifl_create_event_handler at /src/junos/usr.sbin/l2ald/platform/junos/l2ald_rtsock_VXLAN.c:477. [PR1560068](#)
- global-mac-ip-table-aging-time; change from a high to low value might not take effect. [PR1562925](#)
- dev-longevity l2ald cored @ l2ald_next_bd_member. [PR1570757](#)

Forwarding and Sampling

- The configuration archive transfer-on-commit fails when running Junos OS Release 18.2R3-S6.5. [PR1563641](#)

Interfaces and Chassis

- MAC address entry issue might be observed after the MC-LAG interface. [PR1562535](#)

Layer 2 Features

- On the QFX5110-32Q line of switches, LACP does not come up in the Non-Oversubscribed mode for a set of ports. [PR1563171](#)
- On the QFX5120 devices, packets with VLAN ID 0 are dropped. [PR1566850](#)
- MAC addresses learnt from MC-LAG client device might keep flapping between the ICL interface and MC-AE interface after one child link in MC-AE interface is disabled. [PR1582473](#)

Layer 2 Ethernet Services

- DHCP packet drop might be seen when the DHCP relay is configured on a leaf device. [PR1554992](#)

Platform and Infrastructure

- Console access on backup VC member is not allowed. [PR1530106](#)
- FPC might crash in a scaled-firewall configuration. [PR1586817](#)
- On the QFX5000 line of switches, the egress ACL filter entries is only 512 in Junos OS Release 19.4R1. [PR1472206](#)
- On the QFX10000 device, the chassisd process might generate core files on the backup Routing Engine after commit for 200 seconds due to the following error message: CHASSISD_MAIN_THREAD_STALLED. [PR1481143](#)
- The OSPF neighborhood gets stuck in the Start state after configuring the EVPN-VXLAN. [PR1519244](#)
- Layer 3 classifier takes effect though the Layer 2 classifier is configured. [PR1520570](#)
- Some inter-VLAN traffic flows do not converge after rebooting a spine (QFX10002) device in an EVPN-VXLAN non-collapsed scaled scenario. [PR1522585](#)
- Packet drops might be seen with all commit events with 1G speed configured interface. [PR1524614](#)
- Traffic loss might be observed on interfaces in a VXLAN environment. [PR1524955](#)
- On the QFX5100 Virtual Chassis and Virtual Chassis fan, after NSSU while performing GRES, backup can generate core file and go to the database prompt. [PR1533874](#)
- The dcpfe process might crash and cause FPC to restart due to the traffic burst. [PR1534340](#)
- The interfaces on QFX5100-48T switch might stay up when the peer device is rebooting. [PR1538071](#)

- The BFD neighborship fails with the EVPN_VXLAN configuration after the Layer 2 learning restarts. [PR1538600](#)
- On the QFX10000 devices, the dcpfe process might crash in the specific MAC move cases and traffic loss might be observed in the EVPN-VXLAN scenario. [PR1542709](#)
- FPC(s) may fail to come online when the corresponding power is restored afterward but not present during the power-up stage. [PR1545838](#)
- OSPFv3 session might keep flapping and OSPFv3 hellos might be dropped in the host path. [PR1547032](#)
- On QFX10000 device, traffic might get dropped when the set routing-options forwarding-table no-ecmp-fast-reroute configuration is changed to 128 ECMP entries. [PR1547457](#)
- On the QFX10000 devices, you need to move WRL7 SDK to RCPL31. [PR1547565](#)
- The 40GbE interface might be channelized after restarting the Virtual Chassis member. [PR1548267](#)
- The interface filter with source-port 0 matches everything instead of port 0. [PR1551305](#)
- On the QFX5000 devices, the ARP resolution might fail. [PR1552671](#)
- The interface might not come up with 1G optics. [PR1554098](#)
- Traffic might not passed due to the addition of the VLAN tag 2 while passing through the Virtual Chassis port. [PR1555835](#)
- QFX10002-72Q SNMP walk jnxOperatingEntry show only two PSU even four PSU installed. [PR1555852](#)
- Traffic might be dropped when a firewall filter rule uses the then VLAN action. [PR1556198](#)
- The dcpfe process might crash and restart with a dcpfe core file created while running the Type5 EVPN-VXLAN with 2000 VLANs. [PR1556561](#)
- DHCP Discover packets are not getting flooded with VXLAN configuration. [PR1557049](#)
- The MAC addresses learned in a Virtual Chassis may fail aging out in MAC scaling environment. [PR1558128](#)
- On the QFX5000 devices, the firewall filter might fail. [PR1558320](#)
- On the QFX5120 device, amber LEDs are displayed for the fan modules after upgrading to Junos OS Release 20.2R1. [PR1558407](#)
- On the QFX5110 devices, untagged traffic routed over native-vlan might be dropped. [PR1560038](#)

- PRBS (Pseudo Random Binary Sequence) test on the QFX5200 devices fails for 100GbE interfaces with the default settings. [PR1560086](#)
- Few IPv6 ARP ND fails after loading the base configurations. [PR1560161](#)
- On the QFX5120-48Y devices, the Layer 3 IPv4 traffic issue is observed after loading the non-collapsed type 5 EVPN-VXLAN configuration. [PR1560173](#)
- When configuring the static MAC and static ARP on the EVPN core aggregate interface, the underlay next-hop programming might not be updated in the Packet Forwarding Engine. [PR1561084](#)
- The tunable optics SFP+-10G-T-DWDM-ZR doesn't work on EX/QFX devices. [PR1561181](#)
- PTP BC with G.8275.2.enh profile_2 512 clients does not come up. [PR1561348](#)
- PTP lock status gets stuck at the Acquiring state instead of the Phase Aligned state. [PR1561372](#)
- Firewall filters might not work after unified ISSU. [PR1561690](#)
- On the QFX10000 devices, the dcpfe process might crash during the configuration changes. [PR1561746](#)
- Traffic loss might occur in a large-scaled EVPN scenario when the next-hop type changes between discard and unicast. [PR1562425](#)
- On the QFX5000 devices, port mirroring might not work as expected. [PR1562607](#)
- QFX5110-48s-4c :: ptp traffic-statistics are not as expected. [PR1563876](#)
- Output of "show chassis fpc ether-types" command includes FPC slot number. [PR1564496](#)
- The PFE telemetry data might not be streamed out in QFX-VC. [PR1566528](#)
- On the QFX5100 device, the following internal comment is displayed: Placeholder for QFX platform configuration. [PR1567037](#)
- rpd core at boot time of a device. [PR1567043](#)
- On the QFX10002 devices, discrepancy in inet.1 versus Packet Forwarding Engine reports multicast routes. [PR1567353](#)
- QFX10K: Firewall log incorrectly populating from PFE for IPv6 traffic. [PR1569120](#)
- PTP management message with SMTLV is sent only to the first port number to go active in the member multicast-mode l2-ifl. [PR1571283](#)
- Unexpected packet loss might happen if subunit of the physical interface is deleted. [PR1571286](#)
- DCI traffic loss of 100% observed in transit spine devices. [PR1572238](#)

- Traffic loss might be observed due to dcpfe crash on QFX10002/QFX10008 platforms. [PR1572889](#)
- A high rate of 802.3X Pause Frames are sent out of the Interfaces on QFX10k. [PR1575280](#)
- The dual-speed supported DAC cable (100G to 4x25G Splitter) might not come up on QFX5120-48Y. [PR1576180](#)
- TACACS traffic might be dropped. [PR1578579](#)
- The dcpfe process crashes while checking the virtual tunnel-nh packet status. [PR1580114](#)
- When having analyzers mapped to channelized port then the mirror may not happen properly. [PR1580473](#)
- Kernel issue is observed in telemetry when the set services analytics streaming-server <> <> configuration is present and server is not reachable. [PR1581192](#)
- The switchover might be affected with the shared VXLAN tunnel. [PR1581524](#)
- The l2ald process generates the core file in l2ald_vxlan_ifl_create_event_handler while running the EVPN-VXLAN scripts in VQFX during the PCT submission. [PR1582128](#)
- pciephy and firmware download not working after migration to 6.5.19. [PR1582244](#)
- QFX10K Firewall Filter logs are incorrectly populated with entries for protocol 8847. [PR1582780](#)
- IRB:pings through irb interface is not working. [PR1582989](#)
- Port-Mirror : When delete AE member(s) then its NOT getting deleted (mirror trunk group) in the hardware for Analyzer input AE. [PR1589579](#)

Routing Protocols

- The fxpc process might crash after flapping the related protocols in the ECMP scenario. [PR1556224](#)
- BGP LU session flap might be seen with the AIGP used scenario. [PR1558102](#)
- On the QFX5110 devices, the ARP resolution might fail if native-vlan-id is configured on the VXLAN interface. [PR1563569](#)
- The dcpfe process might crash when the size of the Local Bias Filter Bitmap string exceeds 256 characters. [PR1568159](#)
- The untagged packets might not work on EX Series platforms. [PR1568533](#)
- The GRE egress traffic might not be forwarded between the different routing-instances. [PR1573411](#)
- The DHCP packets might be dropped by the QFX5000 in the Static VXLAN scenario. [PR1576168](#)

- The dcpfe process might crash when any interface flaps. [PR1579736](#)
- The rpd process might crash after committing with the configured static group 224.0.0.0 [PR1586631](#)
- On the QFX5000 line of switches, the egress ACL filter entries is only 512 in Junos OS Release 19.4R1. [PR1472206](#)
- On the QFX10000 device, the chassisd process might generate core files on the backup Routing Engine after commit for 200 seconds due to the following error message: CHASSISD_MAIN_THREAD_STALLED. [PR1481143](#)
- The OSPF neighborship gets stuck in the Start state after configuring the EVPN-VXLAN. [PR1519244](#)
- Layer 3 classifier takes effect though the Layer 2 classifier is configured. [PR1520570](#)
- Some inter-VLAN traffic flows do not converge after rebooting a spine (QFX10002) device in an EVPN-VXLAN non-collapsed scaled scenario. [PR1522585](#)
- Traffic loss might be observed on interfaces in a VXLAN environment. [PR1524955](#)
- On the QFX5100 Virtual Chassis and Virtual Chassis fan, after NSSU while performing GRES, backup can generate core file and go to the database prompt. [PR1533874](#)
- The dcpfe process might crash and cause FPC to restart due to the traffic burst. [PR1534340](#)
- The interfaces on QFX5100-48T switch might stay up when the peer device is rebooting. [PR1538071](#)
- The BFD neighborship fails with the EVPN_VXLAN configuration after the Layer 2 learning restarts. [PR1538600](#)
- On the QFX10000 devices, the dcpfe process might crash in the specific MAC move cases and traffic loss might be observed in the EVPN-VXLAN scenario. [PR1542709](#)
- FPC(s) may not boot-up on MX960/EX9214 in a certain condition. [PR1545838](#)
- OSPFv3 session might keep flapping and OSPFv3 hellos might be dropped in the host path. [PR1547032](#)
- On QFX10000 device, traffic might get dropped when the set routing-options forwarding-table no-ecmp-fast-reroute configuration is changed to 128 ECMP entries. [PR1547457](#)
- On the QFX10000 devices, you need to move WRL7 SDK to RCPL31. [PR1547565](#)
- The 40GbE interface might be channelized after restarting the Virtual Chassis member. [PR1548267](#)
- The interface filter with source-port 0 matches everything instead of port 0. [PR1551305](#)
- On the QFX5000 devices, the ARP resolution might fail. [PR1552671](#)

- Traffic might not be passed due to the addition of the VLAN tag 2 while passing through the Virtual Chassis port. [PR1555835](#)
- QFX10002-72Q SNMP walk jnxOperatingEntry show only two PSU even four PSU installed. [PR1555852](#)
- Traffic might be dropped when a firewall filter rule uses the then VLAN action. [PR1556198](#)
- The dcpfe process might crash and restart with a dcpfe core file created while running the Type5 EVPN-VXLAN with 2000 VLANs. [PR1556561](#)
- DHCP Discover packets are not getting flooded with VXLAN configuration. [PR1557049](#)
- The MAC addresses learned in a Virtual Chassis may fail aging out in MAC scaling environment. [PR1558128](#)
- On the QFX5000 devices, the firewall filter might fail. [PR1558320](#)
- On the QFX5120 device, amber LEDs are displayed for the fan modules after upgrading to Junos OS Release 20.2R1. [PR1558407](#)
- On the QFX5110 devices, untagged traffic routed over native-vlan might be dropped. [PR1560038](#)
- PRBS (Pseudo Random Binary Sequence) test on the QFX5200 devices fails for 100GbE interfaces with the default settings. [PR1560086](#)
- Few IPv6 ARP ND fails after loading the base configurations. [PR1560161](#)
- On the QFX5120-48Y devices, the Layer 3 IPv4 traffic issue is observed after loading the non-collapsed type 5 EVPN-VXLAN configuration. [PR1560173](#)
- When configuring the static MAC and static ARP on the EVPN core aggregate interface, the underlay next-hop programming might not be updated in the Packet Forwarding Engine. [PR1561084](#)
- The tunable optics SFP+-10G-T-DWDM-ZR doesn't work on EX/QFX devices. [PR1561181](#)
- PTP BC with G.8275.2.enh profile_2 512 clients does not come up. [PR1561348](#)
- PTP lock status gets stuck at the Acquiring state instead of the Phase Aligned state. [PR1561372](#)
- Firewall filters might not work after ISSU. [PR1561690](#)
- On the QFX10000 devices, the dcpfe process might crash during the configuration changes. [PR1561746](#)
- Traffic loss might occur in a large-scaled EVPN scenario when the next-hop type changes between discard and unicast. [PR1562425](#)
- On the QFX5000 devices, port mirroring might not work as expected. [PR1562607](#)

- QFX5110-48s-4c :: ptp traffic-statistics are not as expected. [PR1563876](#)
- Output of "show chassis fpc ether-types" command includes FPC slot number. [PR1564496](#)
- The PFE telemetry data might not be streamed out in QFX-VC. [PR1566528](#)
- On the QFX5100 device, the following internal comment is displayed: Placeholder for QFX platform configuration. [PR1567037](#)
- rpd core at boot time of a device. [PR1567043](#)
- On the QFX10002 devices, discrepancy in inet.1 versus Packet Forwarding Engine reports multicast routes. [PR1567353](#)
- QFX10K: Firewall log incorrectly populating from PFE for IPv6 traffic. [PR1569120](#)
- PTP management message with SMTLV is sent only to the first port number to go active in the member multicast-mode l2-ifl. [PR1571283](#)
- Unexpected packet loss might happen if subunit of the physical interface is deleted. [PR1571286](#)
- DCI traffic loss of 100% observed in transit spine devices. [PR1572238](#)
- Traffic loss might be observed due to dcpfe crash on QFX10002/QFX10008 platforms. [PR1572889](#)
- A high rate of 802.3X Pause Frames are sent out of the Interfaces on QFX10k. [PR1575280](#)
- The dual-speed supported DAC cable (100G to 4x25G Splitter) might not come up on QFX5120-48Y. [PR1576180](#)
- The dcpfe process crashes while checking the virtual tunnel-nh packet status. [PR1580114](#)
- When having analyzers mapped to channelized port then the mirror may not happen properly. [PR1580473](#)
- Kernel issue is observed in telemetry when the set services analytics streaming-server <> <> configuration is present and server is not reachable. [PR1581192](#)
- The switchover might be affected with the shared VXLAN tunnel. [PR1581524](#)
- The l2ald process generates the core file in l2ald_vxlan_ifl_create_event_handler while running the EVPN-VXLAN scripts in VQFX during the PCT submission. [PR1582128](#)
- pciephy and firmware download not working after migration to 6.5.19. [PR1582244](#)
- QFX10K Firewall Filter logs are incorrectly populated with entries for protocol 8847. [PR1582780](#)
- Port-Mirror : When delete AE member(s) then its NOT getting deleted (mirror trunk group) in the hardware for Analyzer input AE. [PR1589579](#)

User Interface and Configuration

- The configuration under groups stanza is not inherited properly. [PR1529989](#)
- set chassis fpc 0 ether-type only applicable for ether index 6 to 27. [PR1565695](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.2R3 documentation for QFX Series switches.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrading Software on QFX Series Switches | 321](#)
- [Installing the Software on QFX10002-60C Switches | 322](#)
- [Installing the Software on QFX10002 Switches | 323](#)
- [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 | 324](#)
- [Installing the Software on QFX10008 and QFX10016 Switches | 326](#)
- [Performing a Unified ISSU | 330](#)
- [Preparing the Switch for Software Installation | 330](#)
- [Upgrading the Software Using Unified ISSU | 331](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 333](#)

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 21.2R3, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS 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 **20.3** in the Release pull-down list to the right of the Software tab on the Download Software page.
4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 20.3 release.

An Alert box appears.

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

A login screen appears.

6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Download the software to a local host.
8. Copy the software to the device or to your internal software distribution site.
9. Install the new jinstall package on the device.

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

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

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-20.3-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 20.3 `jinstall` package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

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

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

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

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

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

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

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-21.2R3.9.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-x86-64-21.2R3.9.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-x86-64-21.2R3.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-x86-64-21.2R3.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-x86-64-21.2R3.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-
x86-64-21.2R3.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-x86-64-20.4R1.n-secure-signed.tgz`.

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

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

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

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

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

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

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

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

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

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

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

Table 14: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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 | 335](#)
- [What's Changed | 343](#)
- [Known Limitations | 348](#)
- [Open Issues | 349](#)
- [Resolved Issues | 353](#)
- [Documentation Updates | 370](#)
- [Migration, Upgrade, and Downgrade Instructions | 370](#)

These release notes accompany Junos OS Release 21.2R3 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 21.2R3 | 335](#)
- [What's New in 21.2R2 | 335](#)
- [What's New in 21.2R1 | 335](#)

There are no new features or enhancements to existing features for SRX Series devices in Junos OS Release 21.2R2.

What's New in 21.2R3

There are no new features or enhancements to existing features for SRX Series devices in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for SRX Series devices in Junos OS Release 21.2R2.

What's New in 21.2R1

IN THIS SECTION

- [Application Identification \(AppID\) | 336](#)
- [Authentication and Access Control | 337](#)
- [Flow-Based and Packet-Based Processing | 338](#)

- Interfaces | 339
- J-Web | 339
- Juniper Advanced Threat Prevention Cloud (ATP Cloud) | 340
- Junos Telemetry Interface | 341
- Network Management and Monitoring | 341
- Software Installation and Upgrade | 341
- Securing GTP and SCTP Traffic | 342
- VPNs | 342

Learn about new features or enhancements to existing features in this release for the SRX Series.

Application Identification (AppID)

- **TLS version 1.3 support for SSL proxy (SRX Series)**—Starting in Junos OS Release 21.2R1, Secure Sockets Layer (SSL) proxy supports the Transport Layer Security (TLS) protocol version 1.3, which provides improved security and better performance. TLS version 1.3 supports the following cipher suites:

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256

[See [SSL Proxy](#).]

- **Application-based multipath routing (AMR) improvements (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, SRX550 HM, and vSRX)**—Starting in Junos OS release 21.2R1, we've introduced the following improvements for AMR:
 - Support for the traffic in reverse direction
 - Queuing mechanism for out-of-order packets at the receiving device
 - Association of AMR rules and service-level agreement (SLA) rules with advanced policy-based routing (APBR) rule in an APBR profile
 - Link selection option that includes overlay interfaces such as GRE and secure tunnel

- Enablement of AMR in one of the two modes—SLA violation mode or standalone mode
- Support for IPv6 traffic
- Support for AMR over IPsec and GRE sessions

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

- **Multicast support in SD-WAN deployments (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX4100, SRX4200, SRX4600, vSRX)**—Starting in Junos OS Release 21.2R1, we've added support for multicast traffic on SRX Series devices in Provider Edge (PE) for SD-WAN deployments. The support for multicast traffic is available when the security device is operating with forwarding option set as flow-based.

Support for multicast traffic results in bandwidth preservation and more efficient traffic flows.

See [[mode \(Security Forwarding Options\)](#) and [Virtual Routing and Forwarding Instances in SD-WAN Deployments](#)].

- **SLA link preference enhancement (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, SLA link preference for security device interfaces supports custom link tags. You can define the link preferences using the preferred-tag and affinity options.

This enhancement allows application traffic to switch from a lower-priority link to a higher-priority link that meets SLA requirements.

[See [Understanding Link-Type Affinity for the Preferred Link](#) and [sla-rule](#).]

- **Application-based load balancing support for APBR (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, security devices support application-based load balancing for advanced policy-based routing (APBR). The APBR achieves load balancing by moving the application traffic in multiple WAN links using user-defined link selection criteria. The link selection criteria for application traffic depends on the link tag and link priority preference settings you defined for the advanced policy-based routing (APBR) interface. The application traffic distribution through the selected links depends on the link weight configuration.

This feature improves the application traffic distribution performance for APBR and application quality of experience (AppQoE).

[See [Advanced Policy-Based Routing](#), [sla-options](#), and [interface](#).]

Authentication and Access Control

- **Unified policy support for firewall user authentication (SRX Series and vSRX)**—Starting in Junos OS Release 21.2R1, we support firewall user authentication in a security policy with dynamic

applications (unified policy). You can configure pass-through or web authentication in the unified policy to restrict or permit users to access network resources.

Firewall user authentication support in the unified policy provides an additional layer of protection in a network with dynamic traffic changes.

[See [Configure Firewall User Authentication with Unified Policies.](#)]

- **Display dynamic-applications and URL category hit counts in a security policy (NFX Series and SRX Series)**—Starting in Junos OS Release 21.2R1, we've enhanced the `show security policies hit-count` command to include the dynamic applications and URL categories options. You can now display the utility rate of the policy according to the number of hits for the dynamic applications and URL categories.

[See [show security policies hit-count.](#)]

- **Support to configure boot order (SRX1500 and SRX4600)**—Starting in Junos OS Release 21.2R1, you can choose to reboot your security devices from a USB device without power cycling. Use the `request system reboot usb` configuration statement to reboot your device from USB. This statement allows your security devices to detect a new USB device with a soft reboot.

[See [request system reboot usb \(SRX Series\).](#)]

Flow-Based and Packet-Based Processing

- **TCP proxy short-circuit (SRX Series)**—Starting in Junos OS Release 21.2R1, for a session with an active TCP proxy plug-in, the SRX Series device disables TCP proxy if there is no further requirement for the TCP proxy plug-in based on the user-defined configuration or the state of the flow. This enhancement significantly improves the session flow performance.
- **Automated Express Path+ (SRX4600, SRX5400, SRX5600, and SRX5800)**—To enable Express Path+ (formerly known as services offloading) in releases before Junos OS Release 21.2R1, administrators need to manually define individual policies that they want to accelerate with network processing (NP) ASICs. Starting in Junos OS Release 21.2R1, administrators can use automated Express Path+ on the listed SRX Series devices to automatically offload all the eligible sessions to the ASIC network processors. This enhancement significantly improves the session flow performance.

Automated Express Path+ requires underlying network processor cache (NP-cache) infrastructure. Starting in Junos OS Release 21.2R1, we've enabled NP-cache by default on the SRX5000 line of devices. Before this release, the SRX4600 had NP-cache enabled by default.

[See [Express Path.](#)]

- **GRE acceleration enhancement (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.2R1, security devices support the existing PMI and GRE acceleration for non software-defined WAN (SD-WAN) deployments.

PMI and GRE acceleration improve GRE and MPLS-over-GRE performance.

[See [gre-performance-acceleration](#) and [show security flow status](#).]

- **Multicast support in SD-WAN deployments (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, we've added support for multicast traffic on security devices in Provider Edge (PE) for SD-WAN deployments. The support for multicast traffic is available when the security device is operating with forwarding option set as flow-based.

Support for multicast traffic results in bandwidth preservation and more efficient traffic flows.

[See [mode \(Security Forwarding Options\)](#) and [Virtual Routing and Forwarding Instances in SD-WAN Deployments](#).]

- **Support for logging and session-close reasons (SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4200, SRX4600, cSRX, and vSRX)**—Starting in Junos OS Release 21.2R1, we've enhanced the logging feature with support for the following flow functions:

- Log for session-update
- Support for 64-bit unified session-id
- Adding new session close reason in session-close log

We've introduced a CLI command `log session-update` that you can use to update the session details.

[See [Information Provided in Session Log Entries for SRX Series Services Gateways](#).]

Interfaces

- **MRU support (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.2R1, you can configure maximum receive unit (MRU) size to accept packet sizes which are bigger than the configured MTU size and configure different values for both MTU and MRU to prevent frequent fragmentation and reassembly of larger packets on the receiving side. You can configure MRU on the `xe`, `ge`, `et`, and `reth` interfaces.

Use the CLI command `mru` under the `edit interfaces reth0 redundant-ether-options` hierarchy level to configure the MRU size in bytes.

[See [mru](#).]

J-Web

- **Enhanced Monitor and IPsec VPN pages (SRX Series)**—Starting in Junos OS Release 21.2R1, we've refreshed the following pages to provide a better experience for you:

Monitor:

- Network is the first submenu.

- Interfaces and DHCP Server Binding are available under Monitor > Network.
- IPsec VPN menu is available under Monitor > Network to display IKE and IPsec VPN security associations (SAs) and statistics information.

IPsec VPN:

- VPN menu is available under the Network tab.
- The new Remote Access column displays remote URLs for Juniper Secure Connect.
- Use **Add** to add a zone when you create or edit a Site-to-Site or Remote Access VPN tunnel interface.

[See [Monitor IPsec VPN](#), [About the IPsec VPN Page](#), and [Create a Site-to-Site VPN](#).]

- **Enhanced dashboard (SRX Series)**—Starting in Junos OS Release 21.2R1, we've enhanced Dashboard with new widgets to provide a better experience for you:
 - Threat Map—Displays the antivirus and IPS events data of the last one hour
 - NAT—Displays the top 10 source and destination translation hits
 - C&C Server and Malware Source Locations—Displays data of the last one hour
 - Incidents By Severity—Displays the top four incidents of data from the last one hour
 - IPsec VPNs (IKE Peers)—Displays the count of IPsec VPN (IKE peers)

[See [Dashboard Overview](#).]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **DNS DGA and tunnel detection (SRX Series)**—Starting in Junos OS Release 21.2R1, you can configure DNS Domain Generation Algorithm (DGA) detection and DNS tunnel detection. This feature enables you to block the malicious domains and DNS-tunneled requests or responses generated by infected hosts and command-and-control (C&C) servers. DGA periodically generates a large number of domain names that are used as rendezvous points (RPs) with their C&C servers. DNS tunneling is a cyberattack method that encodes the data of malicious programs or protocols in DNS queries and responses.

Use the `set security-metadata-streaming policy policy-name detections dga` and `set security-metadata-streaming policy policy-name detections tunneling` commands at the `[edit services]` hierarchy to configure DNS DGA and tunneling detections.

[See [security-metadata-streaming](#).]

Junos Telemetry Interface

NOTE: For Routing Engine telemetry sensors supported by this platform, see [Telemetry Sensor Explorer](#). If any Platform Forwarding Engine sensors have been added for this release, they are listed below

- **New Packet Forwarding Engine core CPU utilization sensor (SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, you can stream Packet Forwarding Engine core CPU utilization sensor data using Junos telemetry interface (JTI) and Remote Procedure Calls (gRPC) to an outside collector.

To access this sensor, use the resource path `/junos/security/spu/cpu/usage/` in subscriptions.

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

Network Management and Monitoring

- **SOAM support (SRX380, SRX300, SRX320, SRX340, SRX345, and SRX550HM)**—Starting in Junos OS Release 21.2R1, you can send delay measurement packets when a CFM session is established on SRX Series devices. We support performance monitoring MIBs that are necessary to manage Service Operation, Administration, and Maintenance (SOAM) performance monitoring functions that are defined in:
 - Service OAM requirements and framework specified by MEF 17
 - Service OAM Performance Monitoring requirements as specified by SOAM-PM
 - Service OAM management objects as specified by MEF 7.1
 - Technical Specification MEF 36

[See [Enterprise-Specific SNMP MIBs Supported by Junos OS](#).]

Software Installation and Upgrade

- **Support of the PXE boot method (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.2R1, we support the Preboot Execution Environment (PXE) boot method. With a PXE boot server, you can prepare an environment to boot devices by using a network interface that is independent of available data storage devices or installed operating systems. A client-enabled system uses a PXE boot to load an OS from a remote server and boot from it. PXE boot uses the standard protocols UDP/IP, Trivial File Transfer Protocol (TFTP), and BOOTP to transfer the image.

[See [Upgrading the Personality of a Device by Using a PXE Boot Server](#).]

Securing GTP and SCTP Traffic

- **Support for rate limiting based on APN-controlled aggregate rate limiting (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 21.2R1, you can apply rate limiting for specific access point names (APNs) by using APN-controlled aggregate rate limiting (ARL). You can also configure APN groups and attach these groups to the GPRS tunneling protocol (GTP) profile for ARL. Configure the `apn-control` statement at the `[edit security gtp]` hierarchy level to enable the various configurations of APN-controlled ARL.

[See [profile \(Security GTP\)](#), [apn-control \(Security GTP\)](#), [apn-control-group \(Security GTP\)](#), [gtp, show security gtp profile](#), [show security gtp counters](#), and [show security gtp](#).]

VPNs

- **AutoVPN PSK support (SRX5000 line of devices with SPC3 card and vSRX running iked)**—To enable the VPN gateway to use a different IKE preshared key (PSK) for authenticating each remote peer, use the new CLI commands `seeded-pre-shared-key ascii-text` or `seeded-pre-shared-key hexadecimal` under the `[edit security ike policy policy_name]` hierarchy level. See [policy](#).

The SRX5000 line of devices with an SPC3 card and vSRX supports AutoVPN PSK only if the `junos-ike-package` is installed.

To enable the VPN gateway to use the same IKE PSK for authenticating all remote peers, use the existing CLI commands `pre-shared-key ascii-text` or `pre-shared-key hexadecimal`.

We also introduce an optional configuration to bypass the IKE ID validation. Use the `general-ikeid` configuration statement under the `[edit security ike gateway gateway_name dynamic]` hierarchy level to bypass the IKE ID validation. If you enable this option, then during authentication of the remote peer, the SRX Series device and vSRX skips the IKE ID validation, and accepts all IKE ID types (hostname, `user@hostname`). See [general-ikeid](#).

[See [AutoVPN on Hub-and-Spoke Devices](#) and [Example: Configuring AutoVPN with Pre-Shared Key](#).]

- **Simplified packet drop identification for IPsec VPN services (SRX1500, SRX320, SRX340, SRX345, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 21.2R1, you can trace packet drop information without committing the configuration by using the `monitor security packet-drop` operational command for IPsec VPN services. This command includes various filters to generate the output fields according to your requirement.

[See [monitor security packet-drop](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 343](#)
- [What's Changed in Release 21.2R2 | 345](#)
- [What's Changed in Release 21.2R1 | 345](#)

Learn about what changed in the Junos OS main and maintenance releases for SRX Series.

What's Changed in Release 21.2R3

IN THIS SECTION

- [Authentication and Access Control | 343](#)
- [General Routing | 343](#)
- [J-Web | 344](#)
- [Network Management and Monitoring | 344](#)

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 \(CLI Procedure\)](#)

[See [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 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.

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

- **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.](#)]

- **Changes to the NETCONF `<edit-config>` RPC response (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<edit-config>` operation returns an error, the NETCONF server does not emit a `<load-error-count>` element in the RPC response. In earlier releases, the `<edit-config>` RPC response includes the `<load-error-count>` element when the operation fails.

What's Changed in Release 21.2R2

IN THIS SECTION

- [J-Web | 345](#)

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."

What's Changed in Release 21.2R1

IN THIS SECTION

- [Interfaces and Chassis | 345](#)
- [Junos XML API and Scripting | 346](#)
- [Network Management and Monitoring | 346](#)
- [VPNs | 347](#)

Interfaces and Chassis

- Unable to Upgrade a Chassis Cluster Using In-Service Software Upgrade (SRX5400)— In chassis cluster mode, the backup router's destination address for IPv4 and IPv6 routers using the commands `edit system backup-router address destination destination-address` and `edit system inet6-backup-router address destination destination-address` must not be same as interface address configured for IPv4 and IPv6 using the commands `edit interfaces interface-name unit logical-unit-number family inet address ipv4-address` and `edit interfaces interface-name unit logical-unit-number family inet6 address ipv6-address`.

[See [Troubleshooting Chassis Cluster Management Issues](#).]

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.](#)]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See [request system scripts refresh-from](#) and [cert-file \(Scripts\).](#)]

Network Management and Monitoring

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, NFX 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.](#)]

- **Changes to <commit> RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server's response for <commit> operations includes the following changes:

- If a successful `<commit>` operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.
- The NETCONF server response emits the `<source-daemon>` element as a child of the `<error-info>` element instead of the `<rpc-error>` element.
- If you also configure the `flatten-commit-results` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server suppresses any `<commit-results>` XML subtree in the response and only emits an `<ok/>` or `<rpc-error>` element.

[See [Configuring RFC-Compliant NETCONF Sessions](#).]

- **New output field added in `show pfe statistics traffic` command (SRX380)**—Starting in Junos OS Release, you'll see Unicast EAPOL in the output of the `show pfe statistics traffic` command.

[See [show-pfe-statistics-traffic](#).]

VPNs

- **View the traffic selector type for an IPsec tunnel (SRX Series and MX Series)**—You can run the `show security ipsec security-associations detail` command to display the traffic selector type for a VPN. The command displays `proxy-id` or `traffic-selector` as a value for the TS Type output field based on your configuration.

[See [show-security-ipsec-security-associations](#).]

- **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

- [General Routing | 348](#)
- [Platform and Infrastructure | 348](#)
- [VPNs | 349](#)

Learn about known limitations in Junos OS Release 21.2R3 for SRX Series devices.

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

General Routing

- Due to enhancements in ApplID starting Junos OS Release 21.1R1, database files are not compatible with earlier releases. Hence, this issue is expected to be seen during downgrade from Junos OS Release 21.1R1 to earlier releases. [PR1554490](#)

Platform and Infrastructure

- For upgrades to Junos OS version 21.2 or higher from Junos OS versions below 21.2, the `no-validate` option needs to be used in the `request system software upgrade` or the `request system software in-service-upgrade (ISSU)` command. Note: This does not apply to SRX300 series and SRX550HM devices.

For the case of ISSU however, the `no-validate` option does not take effect and you need to use the hidden `no-compatibility-check` option instead as a workaround to be able to use ISSU to Junos 21.2 or higher successfully. This issue was fixed in Junos releases 20.3R3-S5, 20.4R3-S4, 21.1R3-S3 and higher releases. [PR1590099](#) and [PR1638499](#)

- On SRX platforms, when performing ISSU to Junos OS release 22.1 or above releases from a pre-22.1 release, ISSU will be aborted with the warning message "ISSU is not supported for Clock Synchronization (SyncE)". As a workaround use the hidden `no-compatibility-check` option in the ISSU command. This issue is resolved in 21.3R3, 21.4R2, 21.4R3 and higher releases. [PR1652838](#)

VPNs

- On SRX5000 line of devices, in some scenario, the device output might display obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. [PR1432925](#)
- In SPC2 and SPC3 mixed-mode HA deployments, tunnel per second (TPS) is getting affected while dead peer detection (DPD) is being served on existing tunnels. This limitation is due to a large chunk of CPU being occupied by infrastructure (gencfg) used by IKED to synchronize its DPD state to the backup nodes. [PR1473482](#)

Open Issues

IN THIS SECTION

- [Flow-Based and Packet-Based Processing | 350](#)
- [General Routing | 350](#)
- [Interfaces and Chassis | 351](#)
- [Intrusion Detection and Prevention \(IDP\) | 351](#)
- [J-Web | 352](#)
- [Platform and Infrastructure | 352](#)
- [Routing Policy and Firewall Filters | 352](#)
- [Routing Protocols | 352](#)
- [Unified Threat Management \(UTM\) | 352](#)
- [User Interface and Configuration | 353](#)
- [VPNs | 353](#)

Learn about open issues Junos OS Release 21.2R3 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.

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](#)
- For accelerated flows such as Express Path, the packet or byte counters in the session close log and show session output take into account only the values that accumulated while traversing the NP. [PR1546430](#)

General Routing

- In Dual CPE scenario, after RGO failover, the best path link status shows as PARTIAL SLA VIOLATED instead of SLA MET due to active probe result gone wrong in certain scenarios. [PR1565777](#)
- When the device is downgraded to a release earlier than Junos OS Release 21.1 and then upgraded again to Junos OS Release 21.1, the appidb tables might not get populated properly and have 0 entries. For such cases, after upgrading, uninstall and reinstall signature package. [PR1567199](#)
- With the Application-Based Multipath Routing enabled, HTTP sessions take approximately 10 minutes to re-establish after a link flap between hub and spoke. [PR1577021](#)
- 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 LSYS and Tenant, Intermittently Security log contents of binary log file in LSYS are not as expected. [PR1587360](#)
- On SRX Series devices, when firewall authentication is configured with pass-through traffic for http or https with user firewall, SRX Series devices will delete the authentication entries post 10 seconds to avoid re-authentication. [PR1588241](#)
- Unexpected port value 0 is seen instead of undefined. [PR1589598](#)
- On SRX345 device, the icmp checksum error and packet drops are observed while doing rapid ping on vdsl interface with MTU 1514. [PR1591230](#)
- There is a behaviour 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](#)

- For Junos OS releases 20.3R3, 20.4R3, 21.1R2, 21.2R1, phone home ZTP is failing on SRX Series devices as phone home client is unable to connect to Phone Home Server or Redirect Server. [PR1598462](#)
- Intermittently the trace messages are not logged on sending multicast traffic. [PR1598930](#)
- 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 Juniper Secure Connect installed CLIENT. [PR1611003](#)
- On SRX Series device with a sig-pack update, if any application is moved to deprecated and if that application was part of any custom group, signature upgrade might fail. Due to this sometimes the apid process might stop. [PR1632205](#)
- LACPD generates core files sometimes when member links are swapped between two reth bundle using rollback operation given that prior to rollback each of the bundle already has maximum number of child links. [PR1632371](#)
- SMTPS sessions are not getting identified when traffic is sent from IXIA (BPS) profile. [PR1635929](#)
- The remote-access-juniper-std license might not get freed up while disconnect or reconnect after RGO failover. [PR1642653](#)

Interfaces and Chassis

- Traffic drop might be seen on irb interface on SRX1500 device for network control forwarding class when verifying dscp classification based on single and multiple code-points. [PR1611623](#)

Intrusion Detection and Prevention (IDP)

- On SRX Series devices, it is unable to use latest signature pack due to IDP DB failing to update. [PR1594283](#)

J-Web

- The Firefox browser displays an unsaved changes error message in the J-Web basic settings page if the autofill logins and passwords option is selected under the browser privacy and security settings. [PR1560549](#)
- UI lists the IPsec VPNs information for uncommitted IPsec VPNs configuration under Monitor -> Network -> IPsec VPN. [PR1576609](#)
- For Dynamic VPN configuration, topology is shown as 'Site to Site / Hub and Spoke' under Monitor -> Network -> IPsec VPN page. [PR1597889](#)

Platform and Infrastructure

- The commit synchronize command fails because the kernel socket gets stuck. [PR1027898](#)
- 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](#)
- The device will be unavailable while performing FIPS 140-2/FIPS 140-3 level 2 internal test on FreeBSD 12 based Junos OS platforms. [PR1623128](#)

Routing Policy and Firewall Filters

- If tunnel inspection policies are defined, VXLAN sessions are not getting established. [PR1604625](#)

Routing Protocols

- The fwauthd core files might be observed when upgrading to Junos OS 21.2R1 release. [PR1588393](#)

Unified Threat Management (UTM)

- There is no counter for juniper-local default action. [PR1570500](#)

User Interface and Configuration

- On all Junos OS and Junos OS Evolved devices, when copy-config, get-configuration, and discard-change RPCs run in two parallel NETCONF sessions and the database is also accessed in parallel by two NETCONF sessions, it leads to database corruption and mgd-related services might crash. [PR1641025](#)

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](#)
- On SRX5000 line of devices, in some scenario, the device output might display 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](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.2R3 | 354](#)
- [Resolved Issues: 21.2R2 | 360](#)
- [Resolved Issues: 21.2R1 | 365](#)

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R3

IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 354](#)
- [Authentication and Access Control | 354](#)
- [Chassis Clustering | 354](#)
- [Flow-Based and Packet-Based Processing | 355](#)
- [General Routing | 355](#)
- [Interfaces and Chassis | 357](#)
- [Intrusion Detection and Prevention \(IDP\) | 357](#)
- [J-Web | 358](#)
- [Network Address Translation \(NAT\) | 358](#)
- [Platform and Infrastructure | 358](#)
- [Routing Policy and Firewall Filters | 358](#)
- [Routing Protocols | 359](#)
- [User Interface and Configuration | 359](#)
- [VPNs | 359](#)

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](#)

Authentication and Access Control

- The authentication delay might occur upto 60 seconds if same user authenticates. [PR1626667](#)

Chassis Clustering

- Secondary node in a chassis cluster might go into reboot loop on SRX Series devices. [PR1606724](#)
- SPU might become offline on standby node after failover in SRX Series devices with chassis cluster. [PR1624262](#)
- BFD over high-availability ICL link might flap. [PR1631938](#)

- Annotate ip command might bring IP monitoring down and both nodes in MNHA mode goes into INELIGIBLE state. [PR1632586](#)

Flow-Based and Packet-Based Processing

- 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](#)
- Packets might not be classified according to the CoS rewrite configuration. [PR1634146](#)
- The process nsd may crash continuously due to failure in creating/reinitializing the file /var/db/ext/monitor-flow-cfg. [PR1638008](#)

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](#)
- 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](#)
- Changes in SNMP traps configuration and data exported for TWAMP. [PR1573169](#)
- The process pkid might generate core files during local certificate enrollment. [PR1573892](#)
- The fxp0 interface of an SRX550 device in cluster might become unreachable from an external network. [PR1575231](#)
- On SRX Series devices with Chassis Cluster, the tcp_timer_keep:Local(0x81100001:60753) Foreign(0x8f100001:33010) is seen in messages log every 80 seconds. [PR1580667](#)
- BGP adjacency might not get established in Layer 2 with IRB scenario. [PR1582871](#)
- 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](#)
- DNS proxy functionality might not work on VRRP interfaces. [PR1607867](#)
- DNS based Seclntel statistics were not populating correctly on SRX Series devices. [PR1611071](#)

- 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](#)
- The new client might not be able to connect using Juniper Secure Connect if the size of INI file content exceeds the maximum INI file size buffer. [PR1613993](#)
- Packet Forwarding Engine might crash and flowd core might be observed when AppQoS is configured. [PR1615797](#)
- On SRX Series devices running DNS security in secure-wire mode, DGA verdicts would not be returned to the device. [PR1616075](#)
- The srpxfe process might stop when the DNS Security feature is enabled. [PR1616171](#)
- On SRX Series devices using On-Box Logging, LLMD write failures may be seen under high load. The output of show security log llmd counters command can be used to view LLMD behaviour. [PR1620018](#)
- Traffic might get dropped due to memory issue on some SRX Series devices. [PR1620888](#)
- The flowd process might stop on SRX Series devices and NFX devices in AppQoS scenarios. [PR1621495](#)
- On SRX Series devices running DNS Security, if a DGA was detected and the action in the configuration was set to permit, under rare circumstances, a log would not be generated by the device. [PR1624076](#)
- A major chassis alarm for Intel NIC Tx port stuck issue is added on SRX4100 and SRX4200 devices. [PR1624078](#)
- In rare circumstances, PKID could stop and generate a core file when there was limited memory available on the Routing Engine. [PR1624613](#)
- Running DNS on all SRX Series devices, a memory leak on Packet Forwarding Engine might occur. [PR1624655](#)
- Core files might be generated on installing IDP security package. [PR1625364](#)
- The flowd process lost heartbeat for 45 consecutive seconds without alarm raised. [PR1625579](#)
- The error might be seen after configuring a unified security policy allowing some app categories. [PR1628202](#)
- 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 may 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](#)
- The srxpfe process might stop on SRX4600 device. [PR1630990](#)
- Reverse DNS Lookups will no longer be stored in the DNSF Cache when using DNS security. [PR1631000](#)
- Tasks of download manager might not be resumed post reboot. [PR1633503](#)
- On SRX Series devices running DNS Security, a dataplane memory leak may occur within the DNSF plugin when entries age-out of the DNSF cache. [PR1633519](#)
- Unable to connect to domain controller on installing Microsoft KB update. [PR1637548](#)
- The error is seen during the NON-ISSU upgrade from Junos OS 15.1 release to Junos OS 18.2 and later releases [PR1639610](#)
- Configuration change during AppQoS session might result in Packet Forwarding Engine stop with flowd process core file. [PR1640768](#)
- The KRT queue might get stuck with the error- ENOMEM -- Cannot allocate memory. [PR1642172](#)
- The Packet Forwarding Engine might stop on Junos OS SRX Series devices. [PR1642914](#)
- On-Box security logs might be not storing the session-id as a 64-bit integer, resulting in incorrect session-id's being present in the on-box logs. [PR1644867](#)
- Issue with the command clear security idp counters packet-log logical-system all. [PR1648187](#)

Interfaces and Chassis

- Members MAC might be different from parent reth0 interface, resulting loss of traffic. [PR1583702](#)
- 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](#)

- SRX Series devices pause while checking the CLI show security idp attack attack-list policy combine-policy command. [PR1616782](#)
- On SRX Series devices, the request security idp pcap-analysis tool has had usability improvements. [PR1617390](#)
- Updating the IDP signature DB may get the upgrade stuck in the state In progress:Performing Offline download. [PR1623857](#)

J-Web

- The error displays your session has expired. click ok to re-login with root user. [PR1611448](#)
- The AM or PM time format is displayed in customize for Last field at Monitor > Logs > All Events. [PR1628649](#)
- The reboot or halt from J-Web might fail on SRX Series devices. [PR1638370](#)

Network Address Translation (NAT)

- New persistent NAT or normal source NAT sessions might fail due to noncleared aged out sessions. [PR1631815](#)

Platform and Infrastructure

- The pppd process might stop after an upgrade on SRX Series devices. [PR1335526](#)
- 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](#)
- SRX accounting and auditd process might not work on secondary node. [PR1620564](#)
- Error message gencfg_cfg_msg_gen_handler drop might be seen after running commit command. [PR1629647](#)
- When route preferred-metric is different for different RPM policies, the same metric is not reflected in routing records. [PR1634129](#)
- SCB reset with Error : zfchip_scan line = 844 name = failed due to PIO errors. [PR1648850](#)

Routing Policy and Firewall Filters

- SSL proxy might not be performed when SSL Proxy profile is referenced in the zone or global policy [PR1608029](#)

- All feeds of category IPFilter might be removed after committing SecIntel related configurations. [PR1611073](#)
- Redundancy might get affected in SRX Chassis Cluster scenario. [PR1618025](#)

Routing Protocols

- The rpd process might stop in a corner case in PIM-SM scenarios. [PR1574731](#)
- Observing commit error while configuring routing-options rib inet6.0 static on all Junos OS platforms. [PR1599273](#)
- Junos OpenSSH leaves a dangling pointer. [PR1612947](#)
- The wrong BGP path might get selected even when a better or preferred route is available. [PR1616595](#)

User Interface and Configuration

- MGD core might be observed upon ISSU upgrade. [PR1632853](#)

VPNs

- The iked process might restart and generate core during session state activation or deactivation. [PR1573102](#)
- The srxpfe process might stop and generate a core file when IPsec VPN is used. [PR1574409](#)
- Certificate identifier length for PKI CMPv2 CA cert is not displayed as expected in certain cases. [PR1589084](#)
- The kmd process might stop with IPsec tunnel enabled on SRX Series devices and vSRX. [PR1599639](#)
- Flowd process might crash and generate a corefile after upgrade. [PR1603670](#)
- Uneven IPsec tunnel distribution might be seen post tunnels re-establishment. [PR1615763](#)
- Traffic over IPsec tunnels may be dropped post control link failure. [PR1627557](#)
- Traffic loss over IPsec tunnel might be seen on SRX Series devices. [PR1628007](#)
- SRX Series devices generate core files after upgrading to any Junos OS release. [PR1628947](#)
- The kmd process might stop if the IKE negotiation fragment packets are missed during initiating an IKE SA rekey. [PR1638437](#)

Resolved Issues: 21.2R2

IN THIS SECTION

- Authentication and Access Control | [360](#)
- Chassis Clustering | [360](#)
- Flow-Based and Packet-Based Processing | [360](#)
- General Routing | [360](#)
- Interfaces and Chassis | [363](#)
- Intrusion Detection and Prevention (IDP) | [363](#)
- J-Web | [363](#)
- Network Address Translation (NAT) | [363](#)
- Platform and Infrastructure | [364](#)
- Routing Policy and Firewall Filters | [364](#)
- Routing Protocols | [364](#)
- User Interface and Configuration | [364](#)
- VPNs | [364](#)

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

- Performance degradation might be observed when power-mode-ipsec is enabled. [PR1599044](#)

General Routing

- SSL-FP Logging for non SNI session. [PR1442391](#)
- 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 show pfe statistics traffic command shows wrong output. [PR1566065](#)
- When using log templates 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 behavior when multiple log profiles are defined. [PR1570105](#)
- Changes in SNMP traps configuration and data exported for TWAMP. [PR1573169](#)
- Traffic is dropped to or through VRRP virtual IP on SRX380 device. [PR1581554](#)
- The srpxfe process might stop on SRX1500 device. [PR1582989](#)
- Packet drop or srpxfe core dump might be observed due to Glacis FPGA limitation. [PR1583127](#)
- 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](#)
- 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 Series devices will only capture flows marked as UNKNOWN or INCONCLUSIVE. [PR1587875](#)
- IP packets might be dropped on SRX Series devices. [PR1588627](#)
- The jsqsyncd process files generation might cause device to panic crash after upgrade. [PR1589108](#)
- The 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 devices. [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](#)
- When combining log profiles and unified policies RT_FLOW_SESSION_DENY logs were not being generated corrected. [PR1594587](#)
- When JDPI inspection-limits are reached, under certain circumstances, classification details were not propagated to interested Layer-7 Services, such as IDP. [PR1595310](#)

- Node1 fpc0 (SPM) goes down after ISSU and RGO failover. [PR1595462](#)
- Jflow V9 application-id record: Network based application recognition value for IPv4 application-id are not as expected. [PR1595787](#)
- Delay might be observed between Services Processing Card failing and failover to other node. [PR1596118](#)
- The flowd process might core dump if application-services security policy is configured. [PR1597111](#)
- AAMW functions will be bypassed on HTTPs after AppID package upgraded to version 3313 or later. [PR1597179](#)
- The srpxfe process might crash and generate a core file post "targeted-broadcast forward-only" interface-config commit. [PR1597863](#)
- The flowd process might generate files if the AppQoS module receiving two packets of a session. [PR1597875](#)
- The flowd process might stop in AppQoS scenarios. [PR1599191](#)
- The httpd-gk process might generate core files when IPsec VPN is configured. [PR1599398](#)
- The CRC/Align errors and Fragment frames seen with traffic against 400G ports. [PR1601151](#)
- Traffic might be dropped at NAT gateway if EIM is enabled. [PR1601890](#)
- 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 crash if the DNS-inspection feature is enabled within SMS. [PR1607251](#)
- Enabling dnsf traceoptions on SRX300 line of devices might result in flowd process stop. [PR1608669](#)
- 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](#)
- 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](#)

Interfaces and Chassis

- IPv4 or IPv6 address from the config 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)

- 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 crash 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](#)
- High RE CPU usage occurs when routing-instance is configured under security idp security-package hierarchy level. [PR1614013](#)

J-Web

- The zone information disappears when functional zone is configured. [PR1594366](#)
- A custom application name contains any is listed under pre-defined applications. [PR1597221](#)
- J-Web might not display customer defined application services if one new policy is created. [PR1599434](#)
- J-web application might stop with httpd core files are generated. [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. [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](#)
- High CPU usage might be seen on some SRX Series devices. [PR1579425](#)

Routing Protocols

- Short multicast packets drop using PIM when multicast traffic received at a non-RPT or SPT interface. [PR1579452](#)
- The fwauthd core files might be observed when upgrading to Junos OS 21.2R1 release. [PR1588393](#)

User Interface and Configuration

- After image upgrade device might fail to come up due to certain configurations. [PR1585479](#)

VPNs

- The iked core during esp session state activation and deactivation after link encryption tunnel is up. [PR1573102](#)
- The iked process might crash when IKEv2 negotiation fails on MX and SRX Series devices. [PR1577484](#)
- 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](#)

Resolved Issues: 21.2R1

IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 365](#)
- [Chassis Clustering | 365](#)
- [Flow-Based and Packet-Based Processing | 365](#)
- [Forwarding and Sampling | 366](#)
- [General Routing | 366](#)
- [Interfaces and Chassis | 368](#)
- [Intrusion Detection and Prevention \(IDP\) | 368](#)
- [J-Web | 368](#)
- [Network Address Translation \(NAT\) | 369](#)
- [Network Management and Monitoring | 369](#)
- [Platform and Infrastructure | 369](#)
- [Routing Policy and Firewall Filters | 369](#)
- [Unified Threat Management \(UTM\) | 370](#)
- [VPNs | 370](#)

Application Layer Gateways (ALGs)

- On all SRX Series devices, if the SIP ALG is enabled, a core file might be generated. [PR1555817](#)

Chassis Clustering

- Disabled node on chassis cluster sent out ARP request packets. [PR1548173](#)
- SPU pause might be seen under GPRS tunneling protocol scenario. [PR1559802](#)

Flow-Based and Packet-Based Processing

- Instability with RGs on cluster. [PR1550637](#)
- The `usp_max_tcplib_connection` is not expected on SRX1500, SRX4100, and SRX4200 devices. [PR1563881](#)

- On the SRX platforms, the flowd or srpxfe process might crash when clearing the TCP-Proxy session. Traffic loss might be seen during the flowd or srpxfe process crash and restart. [PR1573842](#)
- On SRX Series devices, the filter from-zone has been added to the utility monitor security packet-drop. [PR1574060](#)

Forwarding and Sampling

- The configuration archive transfer-on-commit fails when running Junos OS Release 18.2R3-S6.5. [PR1563641](#)

General Routing

- The flowd process might generate core files frequently on SRX340. [PR1463689](#)
- Packet drops might be seen with all commit events with 1G speed configured interface. [PR1524614](#)
- The JNH memory leak could be observed on MPCs or MICs. [PR1542882](#)
- The output of the command show services application-identification group detail incorrectly included Micro-Applications (Micro-Apps) in the output of every group. [PR1544727](#)
- The kmd process might stop when the interface flaps. [PR1544800](#)
- SRX1500 reports fans running at over speed. [PR1546132](#)
- On SRX4100 and SRX4200 devices, if PEM0 is removed, the output of jnxOperatingDescr.2 command might be incomplete. [PR1547053](#)
- PKI CMPv2 client certificate enrollment does not work on SRX when using root-CA. [PR1549954](#)
- SRX4600 device might reset and fail to boot due to a failure accessing Solid State Drive (SSD). [PR1551047](#)
- On SRX1500, SRX-SFP-1GE-T (Part#740-013111) for a copper cable might be corrupted after reboot. [PR1552820](#)
- The speed mismatch error is seen while trying to commit reth0 with together-options. [PR1553888](#)
- Application identity unknown packet capture utility does not function on SRX Series devices when enhanced-services mode is enabled. [PR1558812](#)
- The show security log report top session-close group-by application order-by risk top-number 8 where-application-risk high xml encapsulation structure changed and caused script fail. [PR1559013](#)
- The show security log report top idp group-by threat-severity order-by count top-number 5 where-attack command display changes. [PR1560027](#)

- The PIC in SRX5K-SPC3 or MX-SPC3 card might get stuck in offline status after flowd process stops on it. [PR1560305](#)
- The pkid process runs at 100 percent when the device is unable to connect to a particular URL. [PR1560374](#)
- The DNS commands might not be executed and any new configuration might not take effect on connecting the SRX Series device to Juniper Sky ATP. [PR1561169](#)
- The show security log report top session-close group-by application order-by risk top-number 8 where-application-risk high xml encapsulation changed. [PR1561286](#)
- The idpd process might stop when committing IDP configuration under logical systems and tenant systems during RGs failover. [PR1561298](#)
- Fabric probe packets might be processed incorrectly when power-mode-ipsec is enabled. [PR1564117](#)
- The flowd process might pause and generates a core dump if JFlow version 9 is configured. [PR1567871](#)
- Wi-Fi mPIM on SRX Series devices is reaching out to NTP and DNS servers. [PR1569680](#)
- Missing snmp operation state method for power distribution module on SRX5800 and MX960 devices. [PR1570433](#)
- MACsec not using network-control queue. [PR1571977](#)
- Traffic going through the VRRP interface might be dropped when VRRP enabled IRB interface goes down. [PR1572920](#)
- In certain conditions on SRX Series devices, the timer values are updated for an existing fast BFD session, it may cause a fast BFD session deletion on the Packet Forwarding Engine. This will result in BFD session remaining down or Packet Forwarding Engine generates core files occasionally. [PR1578946](#)
- The ipfd process might stop and generate a core file when SecProfiling thread feeds are fetched from policy enforcer. [PR1582454](#)
- On SRX1500 device with AE interface configured, if the IRB interface is also configured and enabled, the srxpfe process might stop. [PR1582989](#)
- The 1G interfaces might not come up after device reboot. [PR1585698](#)
- On all Junos OS devices, the l2ald process pause could be observed on changing the routing-instance from VPLS to non-L2 routing-instance, with same routing-instance name is being used for both VPLS and non-L2 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 are 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 Series devices will only capture flows marked as UNKNOWN or INCONCLUSIVE. [PR1587875](#)
- On SRX Series devices, the pass-through traffic on secure web proxy might fail after rebooting the device. [PR1589957](#)

Interfaces and Chassis

- When SRX Series devices receive proxy ARP requests on VRRP interfaces, SRX Series devices send ARP replies with the underlying interface MAC address. [PR1526851](#)
- Backup Routing Engine or backup node might get stuck in bad status with improper backup-router configuration. [PR1530935](#)
- The configuration check out failed with error message: identical local address found on rt_inst [default], intfs. [PR1581877](#)

Intrusion Detection and Prevention (IDP)

- The greater than or less than symbols are allowed for age-of-attack filter of dynamic attack group configuration. The age-of-attack field in signatures will be changed to CVE dates from activation dates. [PR1397599](#)
- IDP now supports the ability to create dynamic-attack-groups based on attack-prefix wildcards. [PR1537195](#)
- Adding signature in packet drop reason and sending to record packet drops module. [PR1574603](#)
- The IDP policy process might become unresponsive and fail to compile the IDP policy after an IDP automatic update. [PR1577684](#)

J-Web

- J-Web GUI does not allow you to save a rule if the cumulative shared objects are more than 2500 before the policy grid is saved. When there are several shared objects, there will be a noticeable delay in opening sources and destinations of a rule, and performing the rule action. [PR1540047](#)
- When the commit pending changes message is shown on the J-Web GUI, the contents of other messages, landing page, or pop-ups will not be clearly visible. [PR1554024](#)

- To improve performance in Monitoring > Network > Interfaces page, Admin Status is removed, services and protocols data merged into one host inbound traffic. [PR1574895](#)

Network Address Translation (NAT)

- Incorrect IPv6 UDP checksum inserted after translation of packet from IPv4 to IPv6, when IPv4 packet did not have a UDP checksum. [PR1596952](#)

Network Management and Monitoring

- The mib2d process crashes and generates a core files on backup Routing Engine. [PR1557384](#)
- SSH connection might become unresponsive and logs show kern.maxfiles limit exceeded by uid messages. [PR1567634](#)

Platform and Infrastructure

- The show chassis errors command is not supported on SRX5000 line of devices with RE3 and SCB3 installed. [PR1560562](#)
- The show chassis ethernet-switch errors command unexpectedly shows error counters for port 14 on the SRX5800 device. [PR1563978](#)
- On SRX5000 line of devices, the power budget calculation incorrectly assumes that all SCB cards contain a Routing Engine (RE). Hence, the available power budget is incorrectly decreased by 90W for each SCB which does not contain an RE. [PR1568183](#)
- There is a limitation where image validation might cause an MGD core thus causing ISSU to abort. This is due to incompatible BSD releases. [PR1590099](#)

Routing Policy and Firewall Filters

- The junos-defaults construct within a unified-policies application match criteria now restricts the ports and protocols of a flow on a per-dynamic-application basis. [PR1551984](#)
- SecIntel connection name resolution errors due to SecIntel memory leaks. [PR1566128](#)
- Traffic loss might be seen when a big number of applications or addresses is referenced by one policy. [PR1576038](#)

Unified Threat Management (UTM)

- UTM license expiry event lost might cause the device can't quit in advance service mode and the maximum-sessions is decreased by half. [PR1563874](#)

VPNs

- Traffic that goes through policy-based IPsec tunnel might be dropped after RGO failover. [PR1550232](#)
- The iked process might stop with Multinode High Availability setup. [PR1559121](#)
- The pkid process generates core files while you do auto-enrollment of local certificates. [PR1564300](#)
- When there are multiple IPsec SAs, backup SA starts IPsec rekey. [PR1565132](#)
- The iked process might crash by operational commands on the SRX5000 line of devices with SRX5000-SPC3 card installed. [PR1566649](#)
- On all SRX Series devices and NFX350, if IPsec tunnels are configured with configuration payload VPN, they might not come up if the configured subnet mask on st0 is not equal to /8, /16 or /24. [PR1593408](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.2R3 documentation for SRX Series.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 371](#)

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 21.2R3, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS 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 15: 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 | 372](#)
- [What's Changed | 374](#)
- [Known Limitations | 376](#)
- [Open Issues | 376](#)
- [Resolved Issues | 377](#)
- [Documentation Updates | 379](#)
- [Upgrade Instructions | 379](#)

These release notes accompany Junos OS Release 21.2R3 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 in 21.2R3 | 372](#)
- [What's New in 21.2R2 | 373](#)
- [What's New in 21.2R1 | 373](#)

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

What's New in 21.2R3

There are no new features or enhancements to existing features for vMX in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for vMX in Junos OS Release 21.2R2.

What's New in 21.2R1

IN THIS SECTION

- [Layer 2 VPN | 373](#)
- [Routing Options | 373](#)
- [Routing Protocols | 374](#)

Learn about new features or enhancements to existing features in this release for the vMX.

Layer 2 VPN

- **Support for Layer 2 services on SR-TE tunnels using transport class (MX series, PTX Series, and vMX)**
—Starting in Junos OS Release 21.2R1, you can configure the following Layer 2 services on colored and non-colored segment routing traffic engineer (SR-TE) tunnels using transport classes.
 - Layer 2 Circuits
 - Layer 2 VPN
 - BGP VPLS

[See [Layer 2 Circuit Overview](#), [Introduction to Configuring Layer 2 VPNs](#), and [BGP Classful Transport Planes Overview](#) .]

Routing Options

- **Forwarding class counters support for flat-file-profile (MX Series and vMX)**—Starting in Junos OS Release 21.2R1, the flat-file-profile statement supports forwarding class counters. You can now switch from the ingress CoS queue counters configuration to the forwarding class counters configuration. To enable the forwarding class counters feature, configure the use-fc-ingress-stats statement at the [edit accounting-options flat-file-profile *profile-name*] hierarchy level.

[See [flat-file-profile \(Accounting Options\)](#).]

Routing Protocols

- **BMP with BGP sharding and update I/O (JRR Series, MX Series, PTX Series, and vMX)**—Starting in Junos OS Release 21.2R1, we support BGP Monitoring Protocol (BMP) with BGP sharding and update I/O in the multithreaded mode.

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 374](#)
- [What's Changed in Release 21.2R2 | 375](#)
- [What's Changed in Release 21.2R1 | 375](#)

Learn about what changed in the Junos OS main and maintenance releases for vMX.

What's Changed in Release 21.2R3

IN THIS SECTION

- [Network Management and Monitoring | 374](#)

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.](#)]

- **Changes to the NETCONF `<edit-config>` RPC response (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<edit-config>` operation returns an error, the NETCONF server does not emit a `<load-error-count>` element in the RPC response. In earlier releases, the `<edit-config>` RPC response includes the `<load-error-count>` element when the operation fails.

What's Changed in Release 21.2R2

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R2 for vMX.

What's Changed in Release 21.2R1

IN THIS SECTION

- [Junos XML API and Scripting | 375](#)
- [Network Management and Monitoring | 376](#)

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python op scripts (ACX Series, EX Series, MX 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.](#)]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the

server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See [request system scripts refresh-from](#) and [cert-file \(Scripts\)](#).]

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](#).]

Known Limitations

There are no known limitations for vMX in Junos OS Release 21.2R3.

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

- [Platform and Infrastructure | 377](#)

Learn about open issues Junos OS Release 21.2R3 for vMX.

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

Platform and Infrastructure

- On vMX, the blockpointer in the ktree is getting corrupted leading to core file generation. There is no function impact such as fpc restart or system down and the issue is not seen in hardware setups. [PR1525594](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.2R3 | 377](#)
- [Resolved Issues: 21.2R2 | 378](#)
- [Resolved Issues: 21.2R1 | 378](#)

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R3

IN THIS SECTION

- [Platform and Infrastructure | 378](#)

Platform and Infrastructure

- On vMX, the traceroute status becomes unhelpful sometimes. [PR1604317](#)
- CFM enhanced SLA iterators monitoring might stop after restarting chassis-control daemon in vMX. [PR1622081](#)
- The vmxt_lnx process generates core files. [PR1638166](#)

Resolved Issues: 21.2R2

IN THIS SECTION

- [Platform and Infrastructure | 378](#)

Platform and Infrastructure

- Interface hold-time up does not work on vMX and MX150 devices. [PR1604554](#)
- Commit failure observed with syntax error "error: load failure on translation changes" while applying tunnel interface configs using openconfig CLI. [PR1621369](#)

Resolved Issues: 21.2R1

IN THIS SECTION

- [Platform and Infrstarcture | 378](#)

Platform and Infrstarcture

- Traffic with jumbo frame might be discarded. [PR1548422](#)
- The AFT based line card might occasionally stops during start up, if the aftd-trio process gets multiple resync messages. The line card will then reboot. [PR1567084](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.2R3 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 21.2R3, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

Junos OS Release Notes for vRR

IN THIS SECTION

- [What's New | 380](#)
- [What's Changed | 380](#)
- [Known Limitations | 381](#)
- [Open Issues | 381](#)
- [Resolved Issues | 382](#)
- [Documentation Updates | 383](#)

These release notes accompany Junos OS Release 21.2R3 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 21.2R3 | 380](#)
- [What's New in 21.2R2 | 380](#)
- [What's New in 21.2R1 | 380](#)

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

What's New in 21.2R3

There are no new features or enhancements to existing features for vRR in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for vRR in Junos OS Release 21.2R2.

What's New in 21.2R1

There are no new features or enhancements to existing features for vRR in Junos OS Release 21.2R1.

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 381](#)
- [What's Changed in Release 21.2R2 | 381](#)
- [What's Changed in Release 21.2R1 | 381](#)

Learn about what changed in the Junos OS main and maintenance releases for vRR.

What's Changed in Release 21.2R3

There are no changes in behavior and syntax in Junos OS Releases 21.2R3 for vRR.

What's Changed in Release 21.2R2

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R2 for vRR.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for vRR.

Known Limitations

Learn about known limitations in Junos OS Release 21.2R3 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 21.2R3, see "[Known Limitations](#)" on [page 142](#) for MX Series routers.

Open Issues

There are no known issues in hardware or software in Junos OS Release 21.2R3 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 21.2R3, see "[Open Issues](#)" on [page 146](#) for MX Series routers.

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.2R3 | 382](#)
- [Resolved Issues: 21.2R2 | 383](#)
- [Resolved Issues: 21.2R1 | 383](#)

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

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

Resolved Issues: 21.2R3

IN THIS SECTION

- [Platform and Infrastructure | 382](#)

To learn more about common BGP or routing resolved issues in Junos OS 21.2R3, see "[Resolved Issues: 21.2R3](#)" on [page 163](#) for MX Series routers.

Platform and Infrastructure

- Support for flexible vlan-tagging on SR-IOV interfaces. [PR1541034](#)
- Memory might be exhausted when both the BGP rib-sharding and the BGP Optimal Route Reflection (ORR) enabled. [PR1613104](#)
- The process rpd might stop in BGP rib-sharding scenario. [PR1613723](#)
- The monitor traffic interface doesn't work on em2. [PR1629242](#)
- vRR VM might establish its identity as Olive after a CLI software upgrade. [PR1635950](#)

Resolved Issues: 21.2R2

IN THIS SECTION

- [Platform and Infrastructure | 383](#)

To learn more about common BGP or routing resolved issues in Junos OS 21.2R2, see "[Resolved Issues: 21.2R2](#)" on [page 179](#) for MX Series routers.

Platform and Infrastructure

- Memory might be exhausted when both the BGP rib-sharding and the BGP ORR. [PR1613104](#)

Resolved Issues: 21.2R1

IN THIS SECTION

- [Platform and Infrastructure | 383](#)

To learn more about common BGP or routing resolved issues in Junos OS 21.2R1, see "[Resolved Issues: 21.2R1](#)" on [page 194](#) for MX Series routers.

Platform and Infrastructure

- On the JRR200 devices, the option-60 vendor-class-identifier are not sent during ZTP. [PR1582038](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.2R3 documentation for vRR.

Junos OS Release Notes for vSRX

IN THIS SECTION

- [What's New | 384](#)
- [What's Changed | 388](#)
- [Known Limitations | 390](#)
- [Open Issues | 391](#)
- [Resolved Issues | 392](#)
- [Documentation Updates | 398](#)
- [Migration, Upgrade, and Downgrade Instructions | 399](#)

These release notes accompany Junos OS Release 21.2R3 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 21.2R3 | 384](#)
- [What's New in 21.2R2 | 385](#)
- [What's New in 21.2R1 | 385](#)

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

What's New in 21.2R3

There are no new features or enhancements to existing features for vSRX in Junos OS Release 21.2R3.

What's New in 21.2R2

There are no new features or enhancements to existing features for vSRX in Junos OS Release 21.2R2.

What's New in 21.2R1

IN THIS SECTION

- [Application Identification \(AppID\) | 385](#)
- [Flow-Based and Packet-Based Processing | 386](#)
- [Platform and Infrastructure | 386](#)
- [Securing GTP and SCTP Traffic | 387](#)
- [VPNs | 387](#)

Learn about new features or enhancements to existing features in this release for the vSRX.

Application Identification (AppID)

- **Multicast support in SD-WAN deployments (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX4100, SRX4200, SRX4600, vSRX)**—Starting in Junos OS Release 21.2R1, we've added support for multicast traffic on SRX Series devices in Provider Edge (PE) for SD-WAN deployments. The support for multicast traffic is available when the security device is operating with forwarding option set as flow-based.

Support for multicast traffic results in bandwidth preservation and more efficient traffic flows.

See [[mode \(Security Forwarding Options\)](#) and [Virtual Routing and Forwarding Instances in SD-WAN Deployments](#)].

- **SLA link preference enhancement (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, SLA link preference for security device interfaces supports custom link tags. You can define the link preferences using the preferred-tag and affinity options.

This enhancement allows application traffic to switch from a lower-priority link to a higher-priority link that meets SLA requirements.

[See [Understanding Link-Type Affinity for the Preferred Link](#) and [sla-rule](#).]

- **Application-based load balancing support for APBR (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—

Starting in Junos OS Release 21.2R1, security devices support application-based load balancing for advanced policy-based routing (APBR). The APBR achieves load balancing by moving the application traffic in multiple WAN links using user-defined link selection criteria. The link selection criteria for application traffic depends on the link tag and link priority preference settings you defined for the advanced policy-based routing (APBR) interface. The application traffic distribution through the selected links depends on the link weight configuration.

This feature improves the application traffic distribution performance for APBR and application quality of experience (AppQoE).

[See [Advanced Policy-Based Routing](#), [sla-options](#), and [interface](#).]

Flow-Based and Packet-Based Processing

- **Support for logging and session-close reasons (SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4200, SRX4600, cSRX, and vSRX)**—Starting in Junos OS Release 21.2R1, we've enhanced the logging feature with support for the following flow functions:
 - Log for session-update
 - Support for 64-bit unified session-id
 - Adding new session close reason in session-close log

We've introduced a CLI command `log session-update` that you can use to update the session details.

[See [Information Provided in Session Log Entries for SRX Series Services Gateways](#).]

Platform and Infrastructure

- **Mellanox support (vSRX 3.0)**—Starting in Junos OS Release 21.2R1, vSRX 3.0 instances that you deploy on VMware and kernel-based virtual machine (KVM) support the Mellanox ConnectX-4 and ConnectX-5 family adapters.

[See [vSRX Deployment for KVM](#).]

- **DPDK version upgrade (vSRX 3.0)**—Starting in Junos OS Release 21.2R1, we've upgraded the Data Plane Development Kit (DPDK) from version 18.11 to version 20.11. The new version supports ICE Poll Mode Driver (PMD), which enables the physical Intel E810 series 100G NIC support on vSRX 3.0.

In this release, Junos FreeBSD 12.X is vSRX 3.0 VM's guest OS. The Routing Engine and Packet Forwarding Engine run on Junos FreeBSD OS as one VM, and the Packet Forwarding Engine utilizes DPDK technologies such as DPDK ICE PMD and single-root I/O virtualization (SR-IOV).

[See [vSRX Deployment for KVM](#).]

Securing GTP and SCTP Traffic

- **Support for rate limiting based on APN-controlled aggregate rate limiting (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 21.2R1, you can apply rate limiting for specific access point names (APNs) by using APN-controlled aggregate rate limiting (ARL). You can also configure APN groups and attach these groups to the GPRS tunneling protocol (GTP) profile for ARL. Configure the `apn-control` statement at the `[edit security gtp]` hierarchy level to enable the various configurations of APN-controlled ARL.

[See [profile \(Security GTP\)](#), [apn-control \(Security GTP\)](#), [apn-control-group \(Security GTP\)](#), [gtp, show security gtp profile](#), [show security gtp counters](#), and [show security gtp](#).]

VPNs

- **AutoVPN PSK support (SRX5000 line of devices with SPC3 card and vSRX running iked)**—To enable the VPN gateway to use a different IKE preshared key (PSK) for authenticating each remote peer, use the new CLI commands `seeded-pre-shared-key ascii-text` or `seeded-pre-shared-key hexadecimal` under the `[edit security ike policy policy_name]` hierarchy level. See [policy](#).

The SRX5000 line of devices with an SPC3 card and vSRX supports AutoVPN PSK only if the `junos-ike-package` is installed.

To enable the VPN gateway to use the same IKE PSK for authenticating all remote peers, use the existing CLI commands `pre-shared-key ascii-text` or `pre-shared-key hexadecimal`.

We also introduce an optional configuration to bypass the IKE ID validation. Use the `general-ikeid` configuration statement under the `[edit security ike gateway gateway_name dynamic]` hierarchy level to bypass the IKE ID validation. If you enable this option, then during authentication of the remote peer, the SRX Series device and vSRX skips the IKE ID validation, and accepts all IKE ID types (hostname, `user@hostname`). See [general-ikeid](#).

[See [AutoVPN on Hub-and-Spoke Devices](#) and [Example: Configuring AutoVPN with Pre-Shared Key](#).]

- **Simplified packet drop identification for IPsec VPN services (SRX1500, SRX320, SRX340, SRX345, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 21.2R1, you can trace packet drop information without committing the configuration by using the `monitor security packet-drop` operational command for IPsec VPN services. This command includes various filters to generate the output fields according to your requirement.

[See [monitor security packet-drop](#).]

What's Changed

IN THIS SECTION

- [What's Changed in Release 21.2R3 | 388](#)
- [What's Changed in Release 21.2R2 | 389](#)
- [What's Changed in Release 21.2R1 | 389](#)

Learn about what changed in the Junos OS main and maintenance releases for vSRX.

What's Changed in Release 21.2R3

IN THIS SECTION

- [Network Management and Monitoring | 388](#)

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.](#)]

- **Changes to the NETCONF <edit-config> RPC response (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the <edit-config> operation returns an error, the NETCONF server does not emit a <load-error-count> element in the RPC response. In earlier releases, the <edit-config> RPC response includes the <load-error-count> element when the operation fails.

What's Changed in Release 21.2R2

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R2 for vSRX.

What's Changed in Release 21.2R1

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.](#)]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See [request system scripts refresh-from](#) and [cert-file \(Scripts\)](#).]

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](#).]

Known Limitations

IN THIS SECTION

- [Platform and Infrastructure | 390](#)

Learn about known limitations in Junos OS Release 21.2R3 for vSRX.

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

Platform and Infrastructure

- For SaaS DBs among all available links a best path chosen. If the link has no violation, and is the preferred link and has the highest priority among all live links, any further configuration change won't be recognized. The recommendation to the user is to configure all the preferences and priorities during configuration time so that all of it can be properly honored. [PR1559662](#)
- The rpd process stops when the device reboot and or process restart. [PR1567043](#)
- On vSRX3.0, the Layer 2 mode is not supported on SR-IOV interfaces. [PR1584705](#)
- For vSRX3 instance deployed on VMware, if Mellanox SR-IOV is used for revenue ports, adding new Mellanox SR-IOV interfaces or deleting existing ones will result in the change of the ordering of the revenue ports. [PR1620532](#)

Open Issues

IN THIS SECTION

- [Uncategorized](#) | 391
- [J-Web](#) | 392
- [VPNs](#) | 392

Learn about open issues Junos OS Release 21.2R3 for vSRX.

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

Uncategorized

- Tag "RT_FLOW_SESSION_XXX" is missing in stream mode. [PR1565153](#)
- When the device is downgraded to a release earlier than Junos OS Release 21.1 and then upgraded again to Junos OS Release 21.1, the application identification database tables might not get populated properly and have 0 entries. For such cases, after upgrading, uninstall and reinstall the signature package. [PR1567199](#)
- 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 because the master RE and secondary RE are out of syncing dcd.snmp_ix information. [PR1571677](#)
- With ssl-proxy configured along with web-proxy, the client session might not closed on the device even though proxy session ends gracefully. [PR1580526](#)
- On SRX Series device with a sig-pack update, if any application is moved to deprecated and if that application was part of any custom group, signature upgrade might fail. Due to this sometimes the apid process might stop. [PR1632205](#)

J-Web

- If any VPN related configuration changes are done from the CLI and committed, click on the Monitor> Network > IPsec VPN menu to see the latest changes. [PR1571751](#)
- UI lists the IPsec VPNs information for uncommitted IPsec VPNs configuration under Monitor -> Network -> IPsec VPN. [PR1576609](#)

VPNs

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

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 21.2R3 | 393](#)
- [Resolved Issues: 21.2R2 | 395](#)
- [Resolved Issues: 21.2R1 | 397](#)

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R3

IN THIS SECTION

- [Flow-Based and Packet-Based Processing | 393](#)
- [General Routing | 393](#)
- [Infrastructure | 394](#)
- [Interfaces and Chassis | 394](#)
- [Intrusion Detection and Prevention \(IDP\) | 394](#)
- [J-Web | 395](#)
- [Routing Protocols | 395](#)
- [User Interface and Configuration | 395](#)
- [VPNs | 395](#)

Flow-Based and Packet-Based Processing

- On SRX Series devices using Unified Policies with IPv6, when attempting to reject certain dynamic-applications, the flowd process might generate core files. [PR1601806](#)
- Cleartext fragments are not processed by flow. [PR1620803](#)

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](#)
- PKID core during auto-re-enrollment of CMPv2 certificates. [PR1580442](#)
- 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](#)
- High CPU utilisation might be seen when Jflow sampling is configured on vSRX HA setup. [PR1604775](#)

- vSRX might stop forwarding traffic 60 days after Junos 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](#)
- During SaaS probing, due to race condition between APP entry addition and session processing, this core is seen. [PR1622787](#)
- On SRX Series devices running DNS security, if a DGA was detected and the action in the configuration was set to permit, under rare circumstances, a log would not be generated by the device. [PR1624076](#)
- Running DNS on all SRX Series devices, a memory leak on Packet Forwarding Engine might occur. [PR1624655](#)
- The application package installation might fail with error in SRX Series devices. [PR1626589](#)
- vSRX3 on VMware ESXi versions 7.0u2 or 7.0u3 with i40e SR-IOV, traffic stopped after reboot. [PR1627481](#)
- Resource errors in show interfaces extensive command output. [PR1629986](#)
- On SRX Series devices running DNS Security, a dataplane memory leak may occur within the DNSF plugin when entries age-out of the DNSF cache. [PR1633519](#)
- Application group name is not found for micro apps in CLI show output. [PR1640040](#)
- The Packet Forwarding Engine might stop on Junos OS SRX Series devices. [PR1642914](#)

Infrastructure

- The failover process may become slow in a vSRX cluster if the gstatd process stops running. [PR1626423](#)

Interfaces and Chassis

- Static route might not work on vSRX. [PR1613430](#)

Intrusion Detection and Prevention (IDP)

- SRX Series devices pause while checking the CLI show security idp attack attack-list policy combine-policy command. [PR1616782](#)

J-Web

- J-Web might only allow certain types of interfaces to be added in a routing-instance. [PR1637917](#)

Routing Protocols

- The rpd process might generate core files due to memory corruption. [PR1599751](#)
- Memory leak in global data shm process might lead to traffic outage. [PR1626704](#)

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](#)
- The process kmd might stop if the ike gateway is configured with two IP address. [PR1626830](#)

Resolved Issues: 21.2R2

IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 395](#)
- [Authentication and Access Control | 396](#)
- [Flow-Based and Packet-Based Processing | 396](#)
- [General Routing | 396](#)
- [Intrusion Detection and Prevention \(IDP\) | 396](#)
- [Network Address Translation \(NAT\) | 397](#)
- [VPNs | 397](#)

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

- 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](#)
- When using log templates (introduced in 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 behavior when multiple log profiles are defined. [PR1570105](#)
- The srxpfe or flowd process might crash when ATP cloud is used. [PR1573157](#)
- vSRX unreachable over SSH after integration with KMS on AWS. [PR1584415](#)
- When combining log profiles and unified policies RT_FLOW_SESSION_DENY logs were not being generated corrected. [PR1594587](#)
- Jflow V9 application-id record: Network based application recognition value for IPv4 application-id are not as expected. [PR1595787](#)
- AAMW functions will be bypassed on HTTPs after AppID package upgraded to version 3313 or later. [PR1597179](#)
- 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 interface order is random. [PR1604060](#)
- vSRX might stop forwarding traffic 60 days after Junos upgrade due to the trial license expiring. [PR1609551](#)
- The interface speed is limited to 1G on vSRX 2.0. [PR1617397](#)

Intrusion Detection and Prevention (IDP)

- The flowd or srxpfe 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](#)

VPNs

- Unable to set DynamoDB in HSM module. [PR1599069](#)

Resolved Issues: 21.2R1

IN THIS SECTION

- [Flow-Based and Packet-Based Processing | 397](#)
- [General Routing | 397](#)
- [Intrusion Detection and Prevention \(IDP\) | 398](#)
- [J-Web | 398](#)
- [Platform and Infrastructure | 398](#)
- [Routing Protocols | 398](#)

Flow-Based and Packet-Based Processing

- The `flowd` or `srxpfe` process might crash when clearing the TCP proxy session. [PR1573842](#)

General Routing

- Packet drops might be seen with all commit events with 1G speed configured interface. [PR1524614](#)
- The Jflow version 5 functionality will not work correctly due to presence of new license infrastructure that is ported recently to vSRX3.0. [PR1549988](#)
- The `pkid` process runs at 100 percent when the device is unable to connect to a particular URL. [PR1560374](#)
- Fabric probe packets might be processed incorrectly when `power-mode-ipsec` is enabled. [PR1564117](#)
- The `rpdd` process generates core files at boot time of a device. [PR1567043](#)
- The `srxpfe` process might stop and generate a core file during the feed update process. [PR1579631](#)

- When a vSRX was performing DNS sinkholing, the sinkhole response packets that it would generate had incorrect checksums. This would cause the receiving client to drop the packet and not be directed to the vSRX's sinkhole. [PR1582827](#)

Intrusion Detection and Prevention (IDP)

- On vSRX3.0 the attack-group-entries filters direction 0 limit 1 command is not showing expected values. [PR1564761](#)
- Application identification related signatures might not get triggered. [PR1588450](#)

J-Web

- J-Web GUI does not allow you to save a rule if the cumulative shared objects are more than 2500 before the policy grid is saved. When there are several shared objects, there will be a noticeable delay in opening sources and destinations of a rule, and performing the rule action. [PR1540047](#)
- After commit pending changes message is shown, the contents of other messages, landing page, or pop-ups are not visible completely. [PR1554024](#)
- To improve performance in Monitoring > Network > Interfaces page, the admin status is removed, services and protocols data merged into one host inbound traffic. [PR1574895](#)

Platform and Infrastructure

- COS queue egress interface forwarding-class might not work as expected. [PR1538286](#)
- If committing source-address <addr> routing-instance and then delete source-address <addr> in private edit mode, commit fails with warning message. [PR1582529](#)

Routing Protocols

- Traffic might be lost during mirror data transmit from the primary pppd or bfdd. [PR1570228](#)

Documentation Updates

There are no corrections or changes in Junos OS Release 21.2R3 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 | 405](#)

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 21.2R3 for vSRX using J-Web (see [J-Web](#)) or the Junos Space Network Management Platform (see [Junos Space](#)).

Starting in Junos OS release 21.2R3, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS 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 21.2R3 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
21.2K Sep 25 14:15 /var/log/messages.0.gz
27B Sep 25 14:15 /var/log/wtmp.0.gz
27B Sep 25 14:14 /var/log/wtmp.1.gz
3027B Sep 25 14:13 /var/tmp/BSD.var.dist
0B Sep 25 14:14 /var/tmp/LOCK_FILE
666B Sep 25 14:14 /var/tmp/appidd_trace_debug
0B Sep 25 14:14 /var/tmp/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 21.2R3 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```
root@vsvrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsvrx-x86-64-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE.tgz /var/crash/corefiles/
```

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

```
root@vsvrx> request system software add /var/crash/corefiles/junos-vsvrx-
x86-64-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsvrx-x86-64-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING: This package will load JUNOS 21.2 software.
WARNING: It will save JUNOS configuration files, and SSH keys
WARNING: (if configured), but erase all other files and information
WARNING: stored on this machine. It will attempt to preserve dumps
WARNING: and log files, but this can not be guaranteed. This is the
WARNING: pre-installation stage and all the software is loaded when
WARNING: you reboot the system.
Saving the config files ...
Pushing Junos image package to the host...
Installing /var/tmp/install-media-srx-mr-vsvrx-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsvrx-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsvrx-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE-linux.tgz
Setting up Junos host applications for installation ...
=====
Host OS upgrade is FORCED
Current Host OS version: 3.0.4
New Host OS version: 3.0.4
Min host OS version required for applications: 0.2.4
=====
Installing Host OS ...
upgrade_platform: -----
upgrade_platform: Parameters passed:
upgrade_platform: silent=0
upgrade_platform: package=/var/tmp/junos-srx-mr-vsvrx-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE-
```



```

linux.tgz
upgrade_platform: clean install=0
upgrade_platform: clean upgrade=0
upgrade_platform: Need reboot after staging=0
upgrade_platform: -----
upgrade_platform:
upgrade_platform: Checking input /var/tmp/junos-srx-mr-
vsrx-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE-linux.tgz is valid.
upgrade_platform: Backing up boot assets..
cp: omitting directory '.'
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
initrd.cpio.gz: OK
upgrade_platform: Checksum verified and OK...
/boot
upgrade_platform: Backup completed
upgrade_platform: Staging the upgrade package - /var/tmp/junos-srx-mr-
vsrx-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE-linux.tgz..
./
./bzImage-intel-x86-64.bin
./initramfs.cpio.gz
./upgrade_platform
./HOST_COMPAT_VERSION
./version.txt
./initrd.cpio.gz
./linux.checksum
./host-version
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
upgrade_platform: Checksum verified and OK...
upgrade_platform: Staging of /var/tmp/junos-srx-mr-
vsrx-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE-linux.tgz completed
upgrade_platform: System need *REBOOT* to complete the upgrade
upgrade_platform: Run upgrade_platform with option -r | --rollback to rollback the upgrade
Host OS upgrade staged. Reboot the system to complete installation!
WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software rollback'

```

```

WARNING:      command as soon as this operation completes.
NOTICE: 'pending' set will be activated at next reboot...
Rebooting. Please wait ...
shutdown: [pid 13050]
Shutdown NOW!
*** FINAL System shutdown message from root@ ***
System going down IMMEDIATELY
Shutdown NOW!
System shutdown time has arrived\x07\x07

```

If no errors occur, Junos OS reboots automatically to complete the upgrade process. You have successfully upgraded to Junos OS Release 21.2R3 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 21.2-2020-06-06.0_RELEASE_21.2_THROTTLE Kernel 64-bit
JNPR-11.0-20171012.170745_fbsd-
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ # cli
root> show version
Model: vsrx
Junos: 21.2-2020-06-06.0_RELEASE_21.2_THROTTLE
JUNOS OS Kernel 64-bit [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]
JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20171017.110007_ssd-builder_release_174_throttle]

```

```

JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_ssd-builder_release_174_throttle]

```

Validating the OVA Image

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

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

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

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

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

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

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

Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 16: 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.

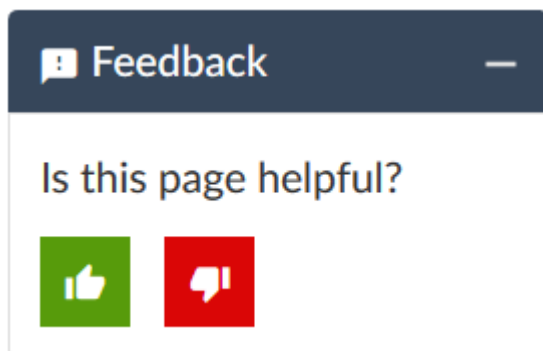
- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#).

<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 | 409](#)
- [Creating a Service Request with JTAC | 409](#)

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/content/dam/www/assets/resource-guides/us/en/jtac-user-guide.pdf>.
- Product warranties—For product warranty information, visit <https://support.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://support.juniper.net/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://support.juniper.net/support/downloads/>
- 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

10 August 2023—Revision 7, Junos OS Release 21.2R3— 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.

20 July 2023—Revision 6, Junos OS Release 21.2R3— 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.

1 June 2023—Revision 5, Junos OS Release 21.2R3— 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 May 2023—Revision 5, Junos OS Release 21.2R3— 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 November 2022—Revision 4, Junos OS Release 21.2R3— 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 3, Junos OS Release 21.2R3— 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.

8 April 2022—Revision 2, Junos OS Release 21.2R3— 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 March 2022—Revision 1, Junos OS Release 21.2R3— 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.

16 November 2021—Revision 1, Junos OS Release 21.2R2— 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.

16 September 2021—Revision 6, Junos OS Release 21.2R1— 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.

26 August 2021—Revision 5, Junos OS Release 21.2R1— 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.

5 August 2021—Revision 4, Junos OS Release 21.2R1- QFX Series.

15 July 2021—Revision 3, Junos OS Release 21.2R1- 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.

8 July 2021—Revision 2, Junos OS Release 21.2R1- 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.

29 June 2021—Revision 1, Junos OS Release 21.2R1- 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.