

Release Notes: Junos[®] OS Release 17.3R3 for the ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion

30 September 2021

Contents	Introduction 11
	Junos OS Release Notes for ACX Series 11
	New and Changed Features 12
	Release 17.3R3 New and Changed Features 12
	Release 17.3R2 New and Changed Features 12
	Release 17.3R1 New and Changed Features 12
	Changes in Behavior and Syntax 14
	General Routing 15
	Interfaces and Chassis 15
	Known Behavior 15
	Known Issues 16
	Class of Service 16
	Hierarchical Class of Service 16
	Interfaces and Chassis 17
	Software Installation and Upgrade 17
	Layer 2 Features 17
	Router 17

Resolved Issues | 18**Resolved Issues: 17.3R3 | 18****Resolved Issues: 17.3R2 | 19****Resolved Issues: 17.3R1 | 19****Documentation Updates | 19****Migration, Upgrade, and Downgrade Instructions | 20****Upgrade and Downgrade Support Policy for Junos OS Releases | 20****Product Compatibility | 21****Hardware Compatibility | 21****Junos OS Release Notes for EX Series Switches | 22****New and Changed Features | 23****Release 17.3R3 New and Changed Features | 24****Release 17.3R2 New and Changed Features | 24****Release 17.3R1 New and Changed Features | 24****Changes in Behavior and Syntax | 31****General Routing | 31****Management | 31****Multicast | 32****Network Management and Monitoring | 32****Routing Protocols | 34****Services Applications | 34****VLAN Infrastructure | 34****Known Behavior | 35****Authentication, Authorization, and Accounting (AAA) (RADIUS) | 35****Platform and Infrastructure | 35****Known Issues | 36****General Routing | 37****High Availability (HA) and Resiliency | 37****Layer 2 Features | 37****Platform and Infrastructure | 37****Virtual Chassis | 38****Resolved Issues | 39****Resolved Issues: 17.3R3 | 39****Resolved Issues: 17.3R2 | 42**

Resolved Issues: 17.3R1	45
Documentation Updates	46
Traffic Management User Guide for EX4600 Switches	46
Migration, Upgrade, and Downgrade Instructions	47
Upgrade and Downgrade Support Policy for Junos OS Releases	47
Product Compatibility	48
Hardware Compatibility	48
Junos OS Release Notes for Junos Fusion Data Center	49
New and Changed Features	49
Changes in Behavior and Syntax	50
Known Behavior	50
Junos Fusion Data Center	50
Known Issues	51
Resolved Issues	52
Resolved Issues: Release 17.3R3	52
Resolved Issues: Release 17.3R2	52
Documentation Updates	53
Migration, Upgrade, and Downgrade Instructions	53
Basic Procedure for Upgrading an Aggregation Device	54
Preparing the Switch for Satellite Device Conversion	56
Autoconverting a Switch into a Satellite Device	58
Manually Converting a Switch into a Satellite Device	61
Configuring a Switch into a Satellite Device Before Connecting It to a Junos Fusion Topology	63
Configuring Satellite Device Upgrade Groups	64
Converting a Satellite Device to a Standalone Device	66
Upgrade and Downgrade Support Policy for Junos OS Releases	68
Downgrading from Release 17.3	68
Product Compatibility	69
Hardware Compatibility	69

Junos OS Release Notes for Junos Fusion Enterprise | 71

New and Changed Features | 71

Junos Fusion Enterprise | 72

Changes in Behavior and Syntax | 73

Junos Fusion Enterprise | 73

Known Behavior | 73

Junos Fusion Enterprise | 74

Known Issues | 74

Junos Fusion Enterprise | 75

Resolved Issues | 75

Resolved Issues: 17.3R3 | 76

Resolved Issues: 17.3R2 | 76

Resolved Issues: 17.3R1 | 77

Documentation Updates | 77

Migration, Upgrade, and Downgrade Instructions | 78

Basic Procedure for Upgrading Junos OS on an Aggregation Device | 78

Upgrading an Aggregation Device with Redundant Routing Engines | 81

Preparing the Switch for Satellite Device Conversion | 81

Converting a Satellite Device to a Standalone Switch | 82

Upgrade and Downgrade Support Policy for Junos OS Releases | 85

Downgrading from Release 17.3 | 85

Product Compatibility | 86

Hardware and Software Compatibility | 86

Hardware Compatibility Tool | 87

Junos OS Release Notes for Junos Fusion Provider Edge | 88

New and Changed Features | 88

Release 17.3R3 New and Changed Features | 89

Release 17.3R2 New and Changed Features | 89

Release 17.3R1 New and Changed Features | 89

Changes in Behavior and Syntax | 90

Known Behavior | 90

Known Issues | 91

Resolved Issues | 92**Resolved Issues: 17.3R3 | 92****Resolved Issues: 17.3R2 | 92****Resolved Issues: 17.3R1 | 93****Documentation Updates | 93****Migration, Upgrade, and Downgrade Instructions | 94****Basic Procedure for Upgrading an Aggregation Device | 94****Upgrading an Aggregation Device with Redundant Routing Engines | 96****Preparing the Switch for Satellite Device Conversion | 97****Converting a Satellite Device to a Standalone Device | 98****Upgrading an Aggregation Device | 100****Upgrade and Downgrade Support Policy for Junos OS Releases | 101****Downgrading from Release 17.3 | 101****Product Compatibility | 102****Hardware Compatibility | 102****Junos OS Release Notes for MX Series 5G Universal Routing Platforms | 103****New and Changed Features | 103****Release 17.3R3-S12 New and Changed Features | 105****Release 17.3R3 New and Changed Features | 105****Release 17.3R2 New and Changed Features | 110****Release 17.3R1 New and Changed Features | 110****Changes in Behavior and Syntax | 135****Class of Service | 136****EVPNs | 136****General Routing | 137****High Availability (HA) and Resiliency | 138****Infrastructure | 138****Interfaces and Chassis | 138****Management | 138****MPLS | 139****Network Management and Monitoring | 140****Routing Protocols | 141****Security | 142****Services Application | 142**

Software Installation and Upgrade	143
Subscriber Management and Services	143
User Interface and Configuration	144
VLAN Infrastructure	145
Known Behavior	145
Class of Service (CoS)	146
EVPN	146
Forwarding and Sampling	148
General Routing	148
High Availability (HA) and Resiliency	150
Infrastructure	150
Interfaces and Chassis	151
MPLS	151
Platform and Infrastructure	152
Routing Protocols	152
Services Application	152
Software Installation and Upgrade	153
Subscriber Management and Services	153
Known Issues	154
Class of Service (CoS)	155
EVPN	155
Forwarding and Sampling	157
General Routing	158
High Availability (HA) and Resiliency	164
Infrastructure	165
Interfaces and Chassis	165
Layer 2 Ethernet Services	166
Layer 2 Features	167
MPLS	167
Platform and Infrastructure	168
Routing Protocols	170
Services Applications	172
Subscriber Access Management	172
User Interface and Configuration	173

VPNs | **173**

Resolved Issues | **174**

Resolved Issues: 17.3R3 | **174**

Resolved Issues: 17.3R2 | **196**

Resolved Issues: 17.3R1 | **209**

Documentation Updates | **214**

Subscriber Management Access Network | **214**

Subscriber Management Provisioning Guide | **214**

Migration, Upgrade, and Downgrade Instructions | **215**

Basic Procedure for Upgrading to Release 17.3 | **216**

Procedure to Upgrade to FreeBSD 10.x based Junos OS | **216**

Procedure to Upgrade to FreeBSD 6.x based Junos OS | **218**

Upgrade and Downgrade Support Policy for Junos OS Releases | **220**

Upgrading a Router with Redundant Routing Engines | **220**

Downgrading from Release 17.3 | **221**

Product Compatibility | **222**

Hardware Compatibility | **222**

Junos OS Release Notes for NFX Series | **223**

New and Changed Features | **223**

Release 17.3R3 New and Changed Features | **224**

Release 17.3R2 New and Changed Features | **224**

Release 17.3R1 New and Changed Features | **224**

Changes in Behavior and Syntax | **224**

Known Behavior | **225**

Known Issues | **225**

Resolved Issues | **226**

Documentation Updates | **226**

Migration, Upgrade, and Downgrade Instructions | **227**

Upgrade and Downgrade Support Policy for Junos OS Releases | **227**

Product Compatibility | **228**

Hardware Compatibility | **228**

Junos OS Release Notes for PTX Series Packet Transport Routers | 229

New and Changed Features | 229

Release 17.3R3 New and Changed Features | 230

Release 17.3R2 New and Changed Features | 230

Release 17.3R1 New and Changed Features | 230

Changes in Behavior and Syntax | 237

Forwarding and Sampling | 238

Interfaces and Chassis | 238

Management | 238

Network Management and Monitoring | 238

Services Application | 239

VLAN-Infrastructure | 240

Known Behavior | 240

General Routing | 240

MPLS | 241

Known Issues | 241

General Routing | 242

Interfaces and Chassis | 243

Routing Protocols | 243

Resolved Issues | 244

Resolved Issues: 17.3R3 | 244

Resolved Issues: 17.3R2 | 246

Resolved Issues: 17.3R1 | 248

Documentation Updates | 249

Migration, Upgrade, and Downgrade Instructions | 249

Upgrade and Downgrade Support Policy for Junos OS Releases | 250

Upgrading a Router with Redundant Routing Engines | 250

Basic Procedure for Upgrading to Release 17.3 | 250

Product Compatibility | 254

Hardware Compatibility | 254

Junos OS Release Notes for the QFX Series | 255

New and Changed Features | 255

Release 17.3R3 New and Changed Features | 256

Release 17.3R2 New and Changed Features | 257

Release 17.3R1 New and Changed Features	258
Changes in Behavior and Syntax	272
Class of Service (CoS)	272
EVPNs	272
General Routing	273
Interfaces and Chassis	273
Management	273
Network Management and Monitoring	274
Routing Policy and Firewall Filters	275
Virtual Chassis	275
VLAN Infrastructure	275
Known Behavior	276
Class of Service (CoS)	277
EVPN	277
High Availability (HA) and Resiliency	278
Layer 2 Features	278
MPLS	278
Platform and Infrastructure	279
Routing Protocols	280
Virtual Chassis	280
Known Issues	281
Class of Service (CoS)	282
EVPN	282
General Routing	282
Interfaces and Chassis	285
Layer 2 Features	285
Network Management and Monitoring	286
Routing Protocols	286
Software Installation and Upgrade	287
Resolved Issues	287
Resolved Issues: 17.3R3	287
Resolved Issues: 17.3R2	293
Resolved Issues: 17.3R1	297

Documentation Updates | 299**Traffic Management User Guide for the QFX Series | 299****Migration, Upgrade, and Downgrade Instructions | 300****Upgrading Software on QFX Series Switches | 300****Installing the Software on QFX10002 Switches | 303****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 | 303****Installing the Software on QFX10008 and QFX10016 Switches | 305****Performing a Unified ISSU | 309****Preparing the Switch for Software Installation | 310****Upgrading the Software Using Unified ISSU | 310****Product Compatibility | 313****Hardware Compatibility | 313****Junos OS Release Notes for SRX Series | 314****New and Changed Features | 314****Release 17.3R2 New and Changed Features | 314****Release 17.3R1 New and Changed Features | 315****Resolved Issues | 320****Resolved Issues: 17.3R2 | 320****Resolved Issues: 17.3R1 | 322****Migration, Upgrade, and Downgrade Instructions | 324****Upgrade and Downgrade Scripts for Address Book Configuration | 324****Product Compatibility | 327****Hardware Compatibility | 328****Upgrading Using Unified ISSU | 329****Compliance Advisor | 329****Finding More Information | 329****Documentation Feedback | 329****Requesting Technical Support | 331****Self-Help Online Tools and Resources | 331****Opening a Case with JTAC | 332****Revision History | 332**

Introduction

Junos OS runs on the following Juniper Networks[®] hardware: ACX Series, EX Series, M Series, MX Series, PTX Series, QFabric systems, QFX Series, SRX Series, T Series, and Junos Fusion.

These release notes accompany Junos OS Release for the ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion. 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

- New and Changed Features | 12
- Changes in Behavior and Syntax | 14
- Known Behavior | 15
- Known Issues | 16
- Resolved Issues | 18
- Documentation Updates | 19
- Migration, Upgrade, and Downgrade Instructions | 20
- Product Compatibility | 21

These release notes accompany Junos OS Release 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.

New and Changed Features

IN THIS SECTION

- [Release 17.3R3 New and Changed Features | 12](#)
- [Release 17.3R2 New and Changed Features | 12](#)
- [Release 17.3R1 New and Changed Features | 12](#)

This section describes the new features or enhancements to existing features in Junos OS Release 17.3R3 for ACX Series Universal Metro Routers.

Release 17.3R3 New and Changed Features

There are no new features or enhancements to existing features in Junos OS Release 17.3R3 for ACX Series Universal Metro Routers.

Release 17.3R2 New and Changed Features

There are no new features or enhancements to existing features in Junos OS Release 17.3R2 for ACX Series Universal Metro Routers.

Release 17.3R1 New and Changed Features

Hardware

- **Support for 100 MB Optics (ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000)**—Starting in Junos OS Release 17.3R1, ACX Series Universal Metro Routers (ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000) support 100 MB Ethernet optics.

[See [Hardware Compatibility Tool](#)]

Class of Service

- **Support for hierarchical class of service (ACX5000)**—Starting in Junos OS Release 17.3R1, ACX5000 line of routers support hierarchical class of service. You can configure up to 8 queues per logical interface. Scheduling properties can be applied at both the physical and logical interface levels. Service providers will be able to support hierarchical class of service at multiple levels to meet the service level agreements and bandwidth allocations for subscribers.

To enable hierarchical scheduling, include the **hierarchical-scheduler** CLI statement at the physical interface level.

Hierarchical class of service can be enabled for Layer 3 VPN, VPLS, and VPWS services.

[See [Hierarchical Class of Service in ACX5000](#).]

Interfaces and Chassis

- **Support for limiting the number of MAC addresses learned from a logical interface (ACX5000)**—Starting in Junos OS Release 17.3R1, you can limit the number of MAC addresses learned from a logical interface on the ACX5000 line of routers. The number of MAC entries learned on a logical interface can be limited by configuring a value for **interface-mac-limit**. The logical interface MAC limit allows the MAC address table space to be distributed among the different logical interfaces. The MAC limiting can be done for both VPLS and VLAN networks. The limits for a bridge domain and logical port can also be configured at the same time.

You can configure MAC address limit by enabling the **set protocols l2-learning global-no-hw-mac-learning** CLI command.

You can specify a limit for MAC addresses at a logical interface level by configuring a value for the **interface-mac-limit** CLI command.

You can use the following show CLI commands to verify this feature:

- **show vlans**
- **show protocols**
- **show routing-instances**
- **show ethernet-switching table**
- **show vpls mac-table**

[See [Configuring MAC Address Limits on a Logical Interface](#).]

- **Support for receiving multicast traffic in a VRF domain (ACX Series)**—Starting in Junos OS Release 17.3R1, ACX Series routers support multicast traffic to be received in a VRF domain.

[See [Configuring an Interface in the VRF Domain to Receive Multicast Traffic](#).]

Timing and Synchronization

- **Support for PTP grandmaster clock (ACX500)**—Starting in Junos OS Release 17.3R1, ACX500 line of routers supports the PTP grandmaster clock functionality. For an ACX500 router to act as a PTP grandmaster clock, the router needs to receive the timing information from a GPS receiver. ACX500 line of routers supports the integrated GNSS receiver, eliminating the need for an external GPS receiver.

NOTE: The grandmaster functionality is supported only on the ACX500 Indoor routers.

[See [Integrated Global Navigation Satellite System \(GNSS\) on ACX500 Series Routers](#) and [IEEE 1588v2 Precision Timing Protocol \(PTP\)](#).]

SEE ALSO

Changes in Behavior and Syntax 14
Known Behavior 15
Documentation Updates 19
Known Issues 16
Resolved Issues 18
Migration, Upgrade, and Downgrade Instructions 20
Product Compatibility 21

Changes in Behavior and Syntax

IN THIS SECTION

- [General Routing | 15](#)
- [Interfaces and Chassis | 15](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 17.3R3 for the ACX Series Universal Metro Routers.

General Routing

- **Support for deletion of static routes when the BFD session goes down (ACX Series)**—Starting with Junos OS Release 17.3R1, the default behavior of the static route at the `[edit routing-options static static-route bfd-admin-down]` hierarchy level is active. So, the static routes are deleted when the BFD receives a session down message.

Interfaces and Chassis

- **Support for logical interfaces**—ACX5048 and ACX5096 routers do not support configuring more than 1000 logical interfaces.

SEE ALSO

New and Changed Features	 12
Known Behavior	 15
Documentation Updates	 19
Known Issues	 16
Resolved Issues	 18
Migration, Upgrade, and Downgrade Instructions	 20
Product Compatibility	 21

Known Behavior

There are no known limitations in Junos OS Release 17.3R3 for the ACX Series.

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

SEE ALSO

New and Changed Features	 12
Changes in Behavior and Syntax	 14
Documentation Updates	 19
Known Issues	 16

[Resolved Issues | 18](#)

[Migration, Upgrade, and Downgrade Instructions | 20](#)

[Product Compatibility | 21](#)

Known Issues

IN THIS SECTION

- [Class of Service | 16](#)
- [Hierarchical Class of Service | 16](#)
- [Interfaces and Chassis | 17](#)
- [Software Installation and Upgrade | 17](#)
- [Layer 2 Features | 17](#)
- [Router | 17](#)

This section lists the known issues in hardware and software in Junos OS Release 17.3R3 for the ACX Series Universal Metro 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

- On ACX5000 line of routers, traffic drop is seen after performing ISSU when class of service is configured. [PR1299539](#)

Hierarchical Class of Service

- On ACX5000 line of routers, whenever you make a change to the queue modes and for the changes to take effect you will need to restart the PFE. [PR1256465](#)
- On ACX5000 line of routers, the **show class-of-service scheduler-hierarchy** CLI command is not supported. [PR1261835](#)
- On ACX5000 line of routers, the **show class-of-service interfaces queue *logical-interface-name*** CLI command does not show **Queue Buffer Usage** for a logical interface. As a workaround, you can use the

PFE shell **show cos halp mmu buffer ifl** command to see the **Queue Buffer Usage** for a logical interface. [PR1272822](#)

- On ACX5000 line of routers, the **shared-buffer maximum** CLI statement for logical interface hierarchical class of service queues does not work correctly. [PR1275796](#)

Interfaces and Chassis

- On ACX Series routers, when link-speed is configured, the aggregate interface goes down permanently after the router reboots. [PR1022248](#)

Software Installation and Upgrade

- ISSU upgrade fails on the ACX5000 line of routers when an AE interface with VLAN map operation **push**, **push-push**, or **pop** is configured in a bridge with no **VLAN ID**. This occurs when the current running Junos OS image is already having an issue, causing the ISSU upgrade to fail. [PR1318771](#)

Layer 2 Features

- On ACX5000 line of routers, in a normal MAC learning mode, when incremental MAC traffic of higher range than the profile is received and after feb restarts, the MAC entries are not seen in the software CLI, although present in the hardware table. As a workaround, in the hardware MAC learning mode, delete the routing instance and reconfigure the routing instance again. In software MAC learning mode, deactivate the routing instance, clear the pending entries or allow the pending entries to be aged out and then activate the routing instance. [PR1277436](#)

Router

- On ACX500 line of routers, performance issues are seen on the ACX500 Indoor AC router. [PR1290278](#)
- On ACX Series routers, at certain instances, the CLI command and syslog shows FAN failure alarms although the fan is running at high speed.

```
user@host> show chassis alarms no-forwarding
alarms currently active
Alarm time           Class  Description
2010-01-01 00:12:04 UTC  Minor  Single FAN Failure

user@host> show chassis environment no-forwarding

Class Item                               Status
```

Measurement		Check	
Fans	Fan 1	OK	Spinning at high speed
	Fan 2		

PR1127846

SEE ALSO

New and Changed Features 12
Changes in Behavior and Syntax 14
Known Behavior 15
Documentation Updates 19
Resolved Issues 18
Migration, Upgrade, and Downgrade Instructions 20
Product Compatibility 21

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 17.3R3 | 18](#)
- [Resolved Issues: 17.3R2 | 19](#)
- [Resolved Issues: 17.3R1 | 19](#)

This section lists the issues fixed in the Junos OS main release and the maintenance releases.

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

Resolved Issues: 17.3R3

There are no fixed issues in Junos OS 17.3R1 for ACX Series.

Resolved Issues: 17.3R2

General Routing

- On ACX Series routers, the DHCP-RELAY requests with IRB interface are not forwarded after upgrade. [PR1243687](#)
- On ACX Series routers, transit ARP packets coming from logical interfaces that are part of a bridge domain or Layer 2 circuit were being sent ("punted") to the Routing Engine. [PR1263012](#)
- On ACX Series router, syslog error was seen on output/egress firewall filter. [PR1316588](#)
- On ACX5000 line of routers, when the management cable was removed, the **Fan & PSU Airflow direction mismatch** major alarm was seen. [PR1327561](#)

Resolved Issues: 17.3R1

Layer 2 Features

- All the XML duplications and unformatted output are addressed. For Example, histogram was just declared as a element inside pfkey container, with this change a new container is defined for histogram. [PR1271648](#)

SEE ALSO

New and Changed Features 12
Changes in Behavior and Syntax 14
Known Behavior 15
Documentation Updates 19
Known Issues 16
Migration, Upgrade, and Downgrade Instructions 20
Product Compatibility 21

Documentation Updates

There are no errata or changes in Junos OS Release 17.3R3 for the ACX Series documentation.

SEE ALSO

New and Changed Features 12

Changes in Behavior and Syntax 14
Known Behavior 15
Known Issues 16
Resolved Issues 18
Migration, Upgrade, and Downgrade Instructions 20
Product Compatibility 21

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases | 20

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL 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://support.juniper.net/support/eol/software/junos/>.

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

SEE ALSO

New and Changed Features	 12
Changes in Behavior and Syntax	 14
Known Behavior	 15
Documentation Updates	 19
Known Issues	 16
Resolved Issues	 18
Product Compatibility	 21

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility](#) | 21

Hardware Compatibility

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.

To determine the features supported on ACX Series routers in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://pathfinder.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

New and Changed Features 12
Changes in Behavior and Syntax 14
Known Behavior 15
Documentation Updates 19
Known Issues 16
Resolved Issues 18
Migration, Upgrade, and Downgrade Instructions 20

Junos OS Release Notes for EX Series Switches

IN THIS SECTION

- New and Changed Features | 23
- Changes in Behavior and Syntax | 31
- Known Behavior | 35
- Known Issues | 36
- Resolved Issues | 39
- Documentation Updates | 46
- Migration, Upgrade, and Downgrade Instructions | 47
- Product Compatibility | 48

These release notes accompany Junos OS Release 17.3R3 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.

New and Changed Features

IN THIS SECTION

- [Release 17.3R3 New and Changed Features | 24](#)
- [Release 17.3R2 New and Changed Features | 24](#)
- [Release 17.3R1 New and Changed Features | 24](#)

This section describes the new features and enhancements to existing features in the Junos OS main release and the maintenance releases for EX Series.

NOTE: The following EX Series switches are supported in Junos OS Release 17.3R3: EX4300, EX4600, and EX9200.

NOTE: In Junos OS Release 17.3R3, J-Web is supported on the EX4300 and EX4600 switches in both standalone and Virtual Chassis setup.

The J-Web distribution model being used provides two packages:

- Platform package—Installed as part of Junos OS; provides basic functionalities of J-Web.
- Application package—Optionally installable package; provides complete functionalities of J-Web.

For details about the J-Web distribution model, see [Release Notes: J-Web Application Package Release 17.3A1 for EX4300 and EX4600 Switches](#).

Release 17.3R3 New and Changed Features

Restoration Procedures and Failure Handling

- **Device recovery mode introduced in Junos OS with upgraded FreeBSD (EX Series)**—Starting in Junos OS Release 17.3R3, for devices running Junos OS with upgraded FreeBSD, there is an automatic device recovery mode that goes into action should the system go into amnesiac mode provided you have saved a rescue configuration on the device. This process enables the system to automatically reboot with the saved rescue configuration. The system displays a banner "Device is in recovery mode" in the CLI in both operational and configuration modes. Previously, there was no automatic process to recover from amnesiac mode. A user with load and commit permission had to log in using the console and fix the issue in the configuration before the system would reboot.

[See [Saving a Rescue Configuration File](#).]

Release 17.3R2 New and Changed Features

There are no new features or enhancements to existing features for EX Series in Junos OS Release 17.3R2.

Release 17.3R1 New and Changed Features

Authentication, Authorization, and Accounting (AAA) (RADIUS)

- **Access control and authentication (EX4600 switches)**—Starting with Junos OS Release 17.3R1, EX4600 switches support controlling access to your network using 802.1X authentication and MAC RADIUS authentication.
 - 802.1X authentication provides port-based network access control (PNAC) as defined in the IEEE 802.1X standard. QFX5100 switches support 802.1X features including guest VLAN, private VLAN, server fail fallback, dynamic changes to a user session, RADIUS accounting, and configuration of port-filtering attributes on the RADIUS server using VSAs. You configure 802.1X authentication at the **[edit protocols dot1x]** hierarchy level.
 - MAC RADIUS authentication is used to authentic end devices independently of whether they are enabled for 802.1X authentication. You can permit end devices that are not 802.1X-enabled to access the LAN by configuring MAC RADIUS authentication on the switch interfaces to which the end devices are connected. You configure MAC RADIUS authentication at the **[edit protocols dot1x authenticator interface interface-name mac-radius]** hierarchy level.
- **IPv6 for RADIUS AAA (EX4300 and EX9200)**—Starting in Junos OS Release 17.3R1, EX4300 and EX9200 switches support IPv6 for user authentication, authorization, and accounting (AAA) using RADIUS servers, in addition to the existing IPv4 support. You can specify which source address Junos OS uses to contact an external RADIUS server. To configure an IPv6 source address for RADIUS authentication, include the source-address statement at the **[edit system radius-server server-address]** hierarchy level. To configure an IPv6 source address for RADIUS accounting, include the source-address statement at the **[edit system accounting destination radius server server-address]** hierarchy level.

NOTE: If an IPv6 RADIUS server is configured without any source-address, default ::0 is considered to be the source address.

[See [source-address](#).]

- **Port bounce with CoA requests and framed-IPv6-address RADIUS attribute for AAA (EX4300 and EX9200)**—Starting in Junos OS Release 17.3R1, the port bounce feature is supported on EX4300 and EX9200 switches. Change of Authorization (CoA) requests are RADIUS messages sent from the authentication, authorization, and accounting (AAA) server to the switch. They are typically used to dynamically change the VLAN for the host based on device profiling. End devices such as printers do not have a mechanism to detect the VLAN change, so they do not renew the lease for their DHCP address in the new VLAN. The port bounce feature is used to force the end device to initiate DHCP re-negotiation by causing a link flap on the authenticated port. There is no configuration required to enable the port bounce feature. Framed-IPv6-Address is an additional RADIUS attribute to support clients with an IPv6 address. The attribute is included in the Access-Request message sent from the client to the AAA server.

[See [Understanding RADIUS-Initiated Changes to an Authorized User Session](#) and [Understanding 802.1X and RADIUS Accounting on Switches](#).]

EVPNs

- **EVPN type-5 route support (EX9200)**—Starting with Junos OS Release 17.3R1, you can configure type-5 routing in an Ethernet VPN (EVPN) environment. Type-5 routing, which advertises IP prefixes through EVPN, is used when the Layer 2 domain does not exist at the remote data centers or metro network peering points.

On EX9200 switches, two models are supported:

- Pure type-5 route without an overlay next hop and type-2 route (MPLS encapsulation only)
- Type-5 route with a gateway IRB interface as an overlay next hop and type-2 route (MPLS and VXLAN encapsulation)

To enable pure type-5 routing, include the **ip-prefix-routes advertise direct-nexthop** statement at the **[edit routing-instances routing-instance-name protocols evpn]** hierarchy level. To enable type-5 routing with a gateway IRB interface, include the **ip-prefix-routes advertise gateway-address** statement at the **[edit routing-instances routing-instance-name protocols evpn]** hierarchy level. Specify a gateway IRB interface by including the **gateway-interface irb-interface-name** statement at the **[edit routing-instances routing-instance-name protocols evpn ip-prefix-routes]** hierarchy level.

[See [ip-prefix-routes](#).]

- **IPv6 support over IRB interfaces for EVPN (EX9200 switches)**—Starting in Junos OS Release 17.3R1, the Ethernet VPN (EVPN) integrated routing and bridging (IRB) solution supports IPv6 and the Neighborhood Discovery Protocol (NDP). NDP is used by IPv6 nodes on the same link to discover each

other's presence, determine each other's Link Layer addresses, find routers, and maintain reachability information about the paths to active neighbors. IPv6 addresses over IRB for EVPN is supported for unique VLAN EVPN instances and for virtual switches with protocol EVPN instances.

[See [EVPN with IRB Solution Overview](#).]

- **EVPN multihoming with ESI per logical interface (EX9200)**—In releases before Junos OS Release 17.3R1, for EX9200 switches, you can configure an Ethernet segment identifier (ESI) only on a physical or aggregated Ethernet interface. In an EVPN-MPLS topology where a customer edge (CE) device is multihomed in active-standby or active-active mode to multiple provider edge (PE) devices, if a physical or aggregated Ethernet interface on an EX9200 switch is considered a non-designated forwarder (DF), the logical interfaces configured on the physical or aggregated Ethernet interface cannot be used for other services. Starting with Junos OS Release 17.3R1 for EX9200 switches, you can now configure an ESI on a logical interface. As a result, even if a logical interface is a non-DF, other logical interfaces on the same physical or aggregated Ethernet interface can still be used for other services.

[See [Example: Configuring an ESI on a Logical Interface for EVPN Multihoming](#).]

- **Layer 3 VXLAN gateway in EVPN-VXLAN topology with a two-layer IP fabric (EX9200)**—Starting with Junos OS Release 17.3R1, EX9200 switches can function as a Layer 3 VXLAN gateway, or spine device, in an EVPN-VXLAN topology with a two-layer IP fabric. In this role, the EX9200 switch uses integrated routing and bridging (IRB) interfaces to route traffic between hosts in different virtual networks (VNs) created by the Contrail virtualization software. When physical (bare-metal) servers in one VN need to communicate with other physical servers or virtual machines (VMs) in another VN, you can also configure an IRB interface as a default Layer 3 gateway that handles the inter-VN traffic for physical servers. In an EVPN-VXLAN topology where a provider edge (PE) device such as a Layer 2 VXLAN gateway or a Contrail vRouter is multihomed in active-active mode to two Layer 3 VXLAN gateways, you can configure redundant default gateways on the Layer 3 VXLAN gateways.

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

Layer 2 Features

- **IRB in PVLAN (EX4600)**—Starting with Junos OS Release 17.3R1, you can configure an IRB interface in a private VLAN (PVLAN) so that devices in the community and isolated VLANs can communicate with each other and with devices outside the PVLAN at Layer 3 without requiring you to install a router.

[See [Example: Configuring a Private VLAN Spanning Multiple Switches with an IRB Interface](#).]

- **PVLAN and Q-in-Q configurations co-exist on a physical interface (EX4600)**—Starting with Junos OS Release 17.3R1, a private VLAN (PVLAN) configuration and a Q-in-Q tunneling configuration can co-exist on the same Ethernet port. Q-in-Q requires a service provider configuration method, and PVLAN requires an enterprise configuration method. To enable both configurations to exist on the same physical interface, you must configure flexible Ethernet services to support dual methods of configuring logical interfaces.

[See [Understanding Flexible Ethernet Services Encapsulation on Switches](#).]

- **L2PT support for tunneling additional protocols (EX9200)**—Starting with Junos OS Release 17.3R1, you can configure Layer 2 protocol tunneling (L2PT) for the following new protocols on EX9200 switches: E-LMI, GVRP, IEEE 802.1X, IEEE802.3AH, LACP, LLDP, MMRP, MVRP, and UDLD.

[See [Layer 2 Protocol Tunneling](#).]

- **L2PT support for tunneling additional protocols (EX4300)**—Starting with Junos OS Release 17.3R1, you can configure Layer 2 protocol tunneling (L2PT) for the following new protocols on EX4300 switches: E-LMI, IEEE 802.1X, MMRP, and UDLD.

[See [Layer 2 Protocol Tunneling](#).]

Layer 3 Features

- **Port-based LAN broadcast traffic forwarding (port helpers) for multiple destination servers (EX9200)**—Starting in Junos OS Release 17.3R1, you can configure port helpers on EX9200 switches with multiple destination servers for a given port. Port helpers listen on configured UDP ports for incoming LAN broadcast traffic, and forward those packets to configured destination servers as unicast traffic. Configure port helpers to listen on a port and forward the traffic to a specified server using the **forwarding-options helpers port port-number** configuration statement with one of the following options:
 - Global—Specify only **server server-ip-address** to listen on *any* interface for the configured port.
 - VLAN-specific—Specify **interface irb-interface-name server server-ip-address** to listen only on a specified IRB interface.
 - Interface-specific—Specify **interface l3-interface-name server server-ip-address** to listen only on a specified Layer 3 interface.

[See [Configuring Port-based LAN Broadcast Packet Forwarding](#).]

Management

- **Support for the Junos Telemetry Interface (EX9200 switches)**—Starting with Junos OS Release 17.3R1, the Junos Telemetry Interface is supported on EX9200 switches. Both UDP and gRPC streaming of statistics are supported. Junos Telemetry Interface enables you to provision sensors to export telemetry data for various network elements without involving polling. The following sensors are supported on EX9200 switches:
 - Aggregated Ethernet interfaces configured with the Link Aggregation Control Protocol (gRPC streaming only)
 - Ethernet interfaces enabled with the Link Layer Discovery Protocol (gRPC streaming only)
 - RSVP interface events (gRPC streaming only)
 - BGP peers (gRPC streaming only)
 - Memory utilization for routing protocol tasks (gRPC streaming only)
 - LSP events and properties (gRPC streaming only)
 - LSP statistics (UDP and gRPC streaming)

- Network Discovery Protocol table state (gRPC streaming only)
- Address Resolution Protocol table state (gRPC streaming only)
- IPFIX inline flow sampling (UDP streaming only)
- Queue depth statistics for ingress and egress queue traffic (UDP streaming only)
- Logical interfaces (UDP and gRPC streaming)
- Firewall filter statistics (UDP and gRPC streaming)
- Optical interfaces (UDP and gRPC streaming)
- Network processing unit (NPU) memory (UDP and gRPC streaming)
- NPU memory utilization (UDP and gRPC streaming)
- CPU memory (UDP and gRPC streaming)
- Fabric statistics (UDP streaming only)
- Physical interfaces (UDP and gRPC streaming)
- Chassis components (gRPC streaming only)

To provision sensors to stream data through UDP, all parameters are configured at the **[edit services analytics]** hierarchy level. To provision sensors to stream data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters for a specified list of OpenConfig command paths. Because EX9200 switches run a version Junos OS with an upgraded FreeBSD kernel, you must download the Junos Network Agent software package, which provides the interfaces to manage gRPC subscriptions. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models.

[See [Overview of the Junos Telemetry Interface](#).]

- **Support for the Junos Telemetry Interface (EX4600 switches)**—Starting with Junos OS Release 17.3R1, you can provision sensors through the Junos Telemetry Interface to export telemetry data for various network elements without involving polling on EX4600 switches. Only gRPC streaming of statistics is supported on EX4600 switches. UDP streaming is not supported.

The following sensors are supported:

- BGP peers
- RSVP interface events
- Memory utilization for routing protocol tasks
- Label-switched-path events and properties
- Ethernet interfaces enabled with the Link Layer Discovery Protocol

To provision sensors to stream data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters for a specified list of OpenConfig commands paths. You must download the Junos Network

Agent software package, which provides the interfaces to manage gRPC subscriptions. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models.

[See [Overview of the Junos Telemetry Interface](#).]

- **Support for Two-Way Active Measurement Protocol (TWAMP) (EX4300 Switches)**—Starting in Junos OS Release 17.3R1, you can measure network performance between any two devices that support the TWAMP protocol. You can use the TWAMP-Control protocol to set up performance measurement sessions and the TWAMP-Test protocol to send and receive performance measurement probes.

You can configure TWAMP to start or stop all of the sessions for all of the TWAMP clients, or start or stop a session for a specific TWAMP client. When you start all the test session configured for a particular TWAMP client, the control-client initiates all requested testing with a Start-Sessions message, and the server sends an acknowledgment. If the control connection is not active between the server and the client, the control connection is also established and the test connections are started later. If the control-client name is not specified, all the configured test sessions are commenced.

When you stop the test session, the control connection is closed only after the Stop-sessions message is sent from the TWAMP client to the TWAMP server. If the control-client name is not specified, all the configured test sessions are closed.

Multiprotocol Label Switching (MPLS)

- **Support for resource RSVP (EX9200)**—Starting in Junos OS Release 17.3R1, the EX9200 switch supports RSVP. RSVP is a signaling protocol that reserves resources, such as for IP unicast and multicast flows, and requests QoS parameters for applications. The protocol was extended with MPLS RSVP-TE to enable RSVP to set up label-switched paths (LSPs) that can be used for traffic engineering in MPLS networks. RSVP is automatically enabled on interfaces on which MPLS-TE is configured. You can enable up to 200 RSVP-TE sessions in the EX9200 advanced feature license (AFL).

[See [RSVP Overview](#) .]

Operation, Administration, and Maintenance

- **Junos OS OpenConfig to support operational models for VLANs (EX Series)**—Starting with Junos OS Release 17.3R1, Junos OS supports an OpenConfig YANG model for VLANs via the addition of **openconfig-vlan.yang**, revision 1.0.2. This provides a unified view for the network agent to retrieve an operational state from Junos OS processes (daemons) for VLANs.

Services Applications

- **Support for enhancing the current inline JFlow scale limits for certain line cards (EX9200-6QS, EX9200-12QS, and EX9200-40XS)**—Starting in Junos OS Release 17.3R1, the **ipv4-flow-table-size** and the **ipv6-flow-table-size** allow up to 256 flow-table-size to support 64M flows at the **[edit chassis fpc slot-number inline-services flow-table-size]** hierarchy level. The existing limit on **flow-export-rate** under **inline-jflow** for each family in the sampling instance is increased to 3200 from 400.

SEE ALSO

Changes in Behavior and Syntax	31
Known Behavior	35
Known Issues	36
Resolved Issues	39
Documentation Updates	46
Migration, Upgrade, and Downgrade Instructions	47
Product Compatibility	48

Changes in Behavior and Syntax

IN THIS SECTION

- General Routing | 31
- Management | 31
- Multicast | 32
- Network Management and Monitoring | 32
- Routing Protocols | 34
- Services Applications | 34
- VLAN Infrastructure | 34

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 17.3R3 for the EX Series.

General Routing

- **Support for deletion of static routes when the BFD session goes down (EX Series)**—Starting with Junos OS Release 17.3R1, the default behavior of the static route at the `[edit routing-options static static-route bfd-admin-down]` hierarchy level is active. So, the static routes are deleted when the BFD receives a session down message. [See [Enabling BFD on Qualified Next Hops in Static Routes for Route Selection.](#)]
- **Enhancement to the show interfaces mc-ae extensive command**—You can now view additional LACP information about the LACP partner system ID when you run the `show interfaces mc-ae extensive` command. The output now displays the following two additional fields:
 - Local Partner System ID-LACP partner system ID as seen by the local node.
 - Peer Partner System ID-LACP partner system ID as seen by the MC-AE peer node.

Previously, the `show interfaces mc-ae extensive` command did not display these additional fields.

[See [show interfaces mc-ae..](#)]

Management

- **Changes to custom YANG RPC syntax (EX Series)**—Starting in Junos OS Release 17.3, custom YANG RPCs have the following changes in syntax:

- The **junos:action-execute** statement is a substatement to **junos:command**. In earlier releases, the **action-execute** and **command** statements are placed at the same level, and the **command** statement is optional.
- The CLI formatting for a custom RPC is defined within the **junos-odl:format** statement, which takes an identifier as an argument. In earlier releases, the CLI formatting is defined using a container that includes the **junos-odl:cli-format** statement with no identifier.
- The **junos-odl:style** statement defines the formatting for different styles within the statement. In earlier releases, the CLI formatting for different styles is defined using a container that includes the **junos-odl:cli-format** and **junos-odl:style** statements.

Multicast

- **Support for per-source multicast traffic forwarding with IGMPv3 (EX4300)**—Starting in Junos OS Release 17.3R3, EX4300 switches forward multicast traffic on a per-source basis according to received IGMPv3 INCLUDE and EXCLUDE reports. In releases prior to this release, EX4300 switches process IGMPv3 reports, but instead of source-specific multicast (SSM) forwarding, they consolidate IGMPv3 INCLUDE and EXCLUDE mode reports for a group into one route for all sources sending to the group. As a result, with the prior behavior, receivers might get traffic from sources they didn't specify.

[See [IGMP Snooping Overview](#).]

Network Management and Monitoring

- **Enhancement to about-to-expire logic for license expiry syslog messages (EX Series)**—Starting in Junos OS Release 17.3R1, the logic for multiple capacity type licenses and when their expiry raises alarms was changed. Before, the behavior had alarms and syslog messages for expiring licenses raised based on the highest validity, which would mislead users in the case of a license expiring earlier than the highest validity license. The new behavior has the about-to-expire logic based on the first expiring license.
- **Change to default log level setting (EX Series)**—Starting in Junos OS Release 17.3R2, changes were made in default logging levels:

Before the change:

- SNMP_TRAP_LINK_UP was LOG_INFO for both the physical (IFD) and logical (IFL) interfaces.
- SNMP_TRAP_LINK_DOWN was LOG_WARNING for both the physical (IFD) and logical (IFL) interfaces.

After the change:

- IFD LinkUp -> LOG_NOTICE (changed because although this is an important message, it occurs very frequently)
- IFL LinkUp -> LOG_INFO (no change)
- IFD and IFL LinkDown -> LOG_WARNING (no change)

[See the [MIB Explorer](#).]

- **Changes to SNMP syslog messages changed (EX Series)**—Starting in Junos OS Release 17.3R1, two misleading SNMP syslog messages have been rewritten to accurately describe the event:
 - OLD --AgentX master agent failed to respond to ping. Attempting to re-register
NEW -- AgentX master agent failed to respond to ping, triggering cleanup!
 - OLD -- NET-SNMP version %s AgentX subagent connected
NEW --- NET-SNMP version %s AgentX subagent Open-Sent!

[See the [MIB Explorer](#).]

- **New context-oid option for trap-options configuration statement distinguishes between traps coming from a non-default routing instance and non-default logical system (EX Series)**—Starting in Junos OS Release 17.3R3, the **context-oid** option for the **trap-options** statement allows you to handle prefixes such as <routing-instance name>@<trap-group> or <logical-system name>/<routing-instance name>@<trap-group> as an additional variable binding.

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

- **Reconfigure SNMPv3 configuration after upgrade (EX4600)**—Starting in Junos OS Release 17.3R1, you might need to reconfigure SNMPv3 after upgrading from an earlier release. This is necessary only if you are using SNMPv3 and if the engine ID is based on the MAC address because the engine ID has changed. Previously, customers had to reconfigure SNMPv3 after every reboot. This problem was fixed. If you upgrade, you must still reconfigure SNMPv3, but only once. If you have already reconfigured SNMPv3 in an earlier release, then you do not need to reconfigure SNMPv3 again. To reconfigure SNMP v3, use the **delete snmp v3** command, commit, and then reconfigure SNMPv3 parameters.

[See [Configuring the Local Engine ID](#).]

Routing Protocols

- **Change in the default behavior of the `advertise-from-main-vpn-tables` configuration statement**—BGP now advertises EVPN routes from the main `bgp.evpn.0` table. You can no longer configure BGP to advertise the EVPN routes from the routing instance table. In earlier Junos OS Releases, BGP advertised EVPN routes from the routing instance table by default.

[See [advertise-from-main-vpn-tables](#).]

Services Applications

- **Changes to the `show services rpm history-results` command (EX Series)**—Starting in Junos OS Release 17.3R2, you must include the **`owner owner`** and **`test name`** options when using the **`show services rpm history-results`** command.

[See [show services rpm history-results](#).]

VLAN Infrastructure

- **LAG interface flaps while adding/removing a VLAN**—From Junos OS Release 17.3 or later, the LAG interface flaps while adding or removing a VLAN. The flapping happens when a low speed SFP is plugged into a relatively high speed port. To avoid flapping, configure the port speed to match the speed of the SFP.

SEE ALSO

[New and Changed Features | 23](#)

[Known Behavior | 35](#)

[Known Issues | 36](#)

[Resolved Issues | 39](#)

[Documentation Updates | 46](#)

[Migration, Upgrade, and Downgrade Instructions | 47](#)

[Product Compatibility | 48](#)

Known Behavior

IN THIS SECTION

- [Authentication, Authorization, and Accounting \(AAA\) \(RADIUS\) | 35](#)
- [Platform and Infrastructure | 35](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 17.3R3 for the EX Series.

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

Authentication, Authorization, and Accounting (AAA) (RADIUS)

- On EX4300 switches, when 802.1X single-supplicant authentication is initiated, multiple "EAP Request Id Frame Sent" packets might be sent. [PR1163966](#)

Platform and Infrastructure

- On EX4600 switches, the amount of time that it takes for Zero Touch Provisioning to complete might be lengthy because TFTP might take a long time to fetch required data. [PR980530](#)

SEE ALSO

- [New and Changed Features | 23](#)
- [Changes in Behavior and Syntax | 31](#)
- [Known Issues | 36](#)
- [Resolved Issues | 39](#)
- [Documentation Updates | 46](#)
- [Migration, Upgrade, and Downgrade Instructions | 47](#)
- [Product Compatibility | 48](#)

Known Issues

IN THIS SECTION

- General Routing | 37
- High Availability (HA) and Resiliency | 37
- Layer 2 Features | 37
- Platform and Infrastructure | 37
- Virtual Chassis | 38

This section lists the known issues in hardware and software in Junos OS Release 17.3R3 for the EX Series.

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

General Routing

- EX9200 is not qualified to support DAC types. [PR1369662](#)

High Availability (HA) and Resiliency

- vmcore on backup Routing Engine though not critical could impact NSR functionality. This can be hit in particular scenarios like: - Back to back GRES with specific configuration. - Commit and rollback the configuration Impact: This will not impact the production Routing Engine since core is on backup. Also, the issue is seen very rarely. Hence, this should not impact the production. [PR1269383](#)

Layer 2 Features

- The eswd process might crash after doing a Routing Engine switchover in an EX Series Virtual Chassis scenario. The crash happens due to a disordered processing of VLAN/vmember by eswd and L2PT modules. As the order of processing does not remain the same every time, the crash is random across switchovers. [PR1275468](#)

Platform and Infrastructure

- On EX4600 and QFX5100 switches, the amount of time that it takes for Zero Touch Provisioning to complete might be lengthy because TFTP might take a long time to fetch required data. [PR980530](#)
- On EX4300, EX4600, and QFX5100 switches, if a remote analyzer has an output IP address that is reachable through a route learned by BGP, the analyzer might be in a DOWN state. [PR1007963](#)
- On chassis based line cards, the **FI: Protect: Parity error for CP freepool SRAM** SRAM parity error might be seen. It's harmless and can be ignored. [PR1079726](#)
- On an EX4300 or a QFX5100 Virtual Chassis, when you perform an NSSU, there might be more than five seconds of traffic loss for multicast traffic. [PR1125155](#)
- On EX4300 switches, when 802.1X single-suplicant authentication is initiated, multiple "EAP Request Id Frame Sent" packets might be sent. [PR1163966](#)
- On an EX9200-12QS line card, interfaces with the default speed of 10-Gigabit Ethernet are not brought down even when the remote end of a connection is misconfigured as 40-Gigabit Ethernet. [PR1175918](#)
- On an EX9200-40XS line card, if you toggle the MACsec encryption option multiple times, encryption and protected MACsec statistics might be updated incorrectly. As a workaround, restart the line card. [PR1185659](#)
- On an EX9200 switch with MC-LAG, when the enhanced-convergence statement is enabled, and when the kernel sends a next hop message to the Packet Forwarding Engine, the full Layer 2 header is not sent and a packet might be generated with an invalid source MAC address for some VLANs. [PR1223662](#)

- On an EX Series switch chassis, if Dynamic Host Configuration Protocol (DHCP) relay or DHCP server is configured along with bpdu-block, a memory allocation issue may be seen. That can lead to a memory exhaustion issue for the DHCP process. [PR1259918](#)
- A flexible VLAN-tagged interface allows both primary and secondary VLAN configuration on different logical units of the same interface, but might not work as expected. [PR1267160](#)
- On EX4300 10G links, preexisting MACsec sessions might not come up after the following events: Process (pfex, dot1x) restart or system restart Link flaps. [PR1294526](#)
- MPC5 inline keepalive PPP echo requests not transmitted when anchor point is lt-x/2/x or lt-x/3/x in pseudowire deployment. [PR1345727](#)
- There are multiple failures when a events like node reboots, ICL flaps and ICCP flaps happens even with enhanced convergence configured there will be no guarantee that sub-second convergence will be achieved. [PR1371493](#)
- Scale of 150 VRRP was not tested before, there are no issues observed for 100 VRRP groups. At the higher scale, there are no drops but traffic gets flooded for group beyond 100. [PR1371520](#)

Virtual Chassis

- When the linecard role FPC is removed and rejoined to the Virtual Chassis immediately, the LAG interface on the master or backup would not be reprogrammed in the rejoined FPC. [PR1255302](#)

SEE ALSO

[New and Changed Features | 23](#)

[Changes in Behavior and Syntax | 31](#)

[Known Behavior | 35](#)

[Resolved Issues | 39](#)

[Documentation Updates | 46](#)

[Migration, Upgrade, and Downgrade Instructions | 47](#)

[Product Compatibility | 48](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 17.3R3 | 39](#)
- [Resolved Issues: 17.3R2 | 42](#)
- [Resolved Issues: 17.3R1 | 45](#)

This section lists the issues fixed in the Junos OS main release and the maintenance releases for EX 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: 17.3R3

EVPN

- The traffic might get dropped as the core is down. [PR1343515](#)

High Availability (HA) and Resiliency

- When **igmp-snooping** and **bpdu-block-on-edge** are enabled, IP protocol multicast traffic sourced by the kernel such as OSPF, VRRP gets dropped in the Packet Forwarding Engine level. [PR1301773](#)

Infrastructure

- PFC feature might not work on an EX4600. [PR1322439](#)
- ifinfo core files can be generated on EX4600 Virtual Chassis. [PR1324326](#)

Interfaces and Chassis

- Identical IP addresses can be configured on different logical interfaces from different physical interfaces in the same routing instance (including master routing instance). [PR1221993](#)
- On an EX4300 Virtual Chassis, an LACP flap is observed after rebooting the master FPC with PDT configurations. [PR1301338](#)
- The interface might not work properly after the FPC restarts. [PR1329896](#)
- The MAC address assigned to an aggregated Ethernet member interface is not the same as that of its parent aggregated Ethernet interface upon master node removal. [PR1333734](#)
- On an EX4600 MC-LAG after reboot of VRRP master and backup black holes traffic to downstream switches. [PR1345316](#)

MPLS

- On EX4600 switches, unified ISSU is not supported with an MPLS configuration. [PR1264786](#)

Platform and Infrastructure

- After access rejected the dot1x process might crash due to a memory leak. [PR1160059](#)
- The **interface-range** command cannot be used to set speed and autonegotiation properties for a group of interfaces. [PR1258851](#)
- The mismatch of VLAN ID between an logical interface and VLAN configuration might result in traffic blackhole. [PR1259310](#)
- EX : Interface does not come up after unplugged/plugged the 1G SFP. [PR1261468](#)
- MACsec session cannot be recovered after physically flapping one link of an aggregated Ethernet. [PR1283314](#)
- Doing load replace terminal and attempting to replace the interface stanza might terminate the current CLI session and leave user session hanging. [PR1293587](#)
- An eswd core file might be observed if apply-groups is configured under interface-range. [PR1300709](#)
- Multicast receiver connected to EX4300 might not be able to get the multicast streaming. [PR1308269](#)
- Autonegotiation is not working as expected between EX4300 and SRX5800. [PR1311458](#)
- JDISwitchingReg : Traffic loss is observed while performing NSSU. [PR1311977](#)
- IGMP snooping might not learn multicast router interface dynamically. [PR1312128](#)
- PEM alarms and L2C failures are observed on MX240/MX480/MX960/EX92/SRX5K devices. [PR1312336](#)
- The interface with 1G SFP might go down if no-auto-negotiation is configured. [PR1315668](#)
- IGMPv3 on an EX4300 does not have the correct outgoing interfaces in the Packet Forwarding Engine that are listed in the kernel. [PR1317141](#)
- The vmcore might be seen and the device might reboot after the ICL is changed from an aggregated Ethernet to a physical interface. [PR1318929](#)
- High latency might be observed between the master Routing Engine and other FPC. [PR1319795](#)
- Multicast traffic might not be forwarded to one of the receivers. [PR1323499](#)
- MAC learning issue and new VLANs creation failure might happen for some VLANs on EX4300 platform. [PR1325816](#)
- EX Series switches do not send RADIUS request after modifying the interface-range configuration. [PR1326442](#)
- An l2cpd process might generate a core file. [PR1325917](#)
- The major alarm about **Fan & PSU Airflow direction mismatch** might be seen by removing management cable. [PR1327561](#)

- Traffic going through aggregated Ethernet interface might be dropped if mastership changes. [PR1327578](#)
- CoS is wrongly applied on Packet Forwarding Engine leading to egress traffic drop. [PR1329141](#)
- [EX4300] When exhausting TCAM table filter is still programmed. [PR1330148](#)
- The rpd process generated a core file on the new backup Routing Engine at **task_quit,task_terminate_timer_callback,task_timer_dispatch,task_scheduler** after disabling NSR+GRES. [PR1330750](#)
- The interface on which the VSTP is disabled by CLI might stay in the "Discarding" state after device rebooting. [PR1333684](#)
- STP BPDUs are not sent out on another active child when an anchor FPC has no active child. [PR1333872](#)
- MQSS errors and alarms might happen when an interface goes down. [PR1334928](#)
- An EX4300 will not generate L2ALD storm control action logs if the interface has a redundant trunk group (RTG) configuration. [PR1335256](#)
- IGMP packets are forwarded out of the RTG backup interface. [PR1335733](#)
- L2cpd memory leak appears on EX platforms with VoIP configured. [PR1337347](#)
- MAC source address filter with the **accept-source-mac** statement does not work if MAC move limit is configured. [PR1341520](#)
- MSTP might not work normally after permitting a commit. [PR1342900](#)
- The filter might not be programmed in Packet Forwarding Engine even though TCAM entries are available. [PR1345296](#)
- Statistics daemon pfd might generate a core file on an upgrade between certain releases. [PR1346925](#)
- After EX9200 FPC becomes Online, other FPC CPU may go 100% usage and have traffic loss near 30sec. [PR1346949](#)
- The VLAN translation feature does not work for the control plane traffic. [PR1348094](#)
- EX4600 detects a Latency-over-Threshold event with a wrong value. [PR1348749](#)
- Traffic drop might happen if LLC packets are sent with DSAP and SSAP as 0x88 and 0x8e. [PR1348618](#)
- Firewall filter with the syslog option is unable to send syslog files to the syslog server running Junos OS Release 16.1R5 or Release 16.1R6 on an EX4300 Virtual Chassis. [PR1351548](#)
- A high usage chassis alarm in "/var" does not clear from the EX4300 Virtual Chassis when a file is copied from fpc1 (master) to fpc0 (backup). [PR1354007](#)
- The ports using SFP-T transceiver might be still up after system halt. [PR1354857](#)
- The FPC would crash due to the memory leak caused by the VTEP traffic. [PR1356279](#)
- MPCs might restart during ISSU. [PR1359282](#)

Routing Protocols

- An mcsnoopd core file is observed at `__raise,abort,__task_quit__,task_quit,task_terminate_timer_callback,task_timer_dispatch,task_scheduler_internal(enable_slip_detector=true,no_exit=true)` at `../src/junos/lib/libtask/base/task_scheduler.c:275`. [PR1305239](#)
- OSPF routes cannot be installed to the routing table until the lsa-refresh timer expires. [PR1316348](#)
- BGP peer is not established after Routing Engine switchover when graceful-restart and BFD enabled. [PR1324475](#)
- The `igmp-snooping` command might be enabled unexpectedly. [PR1327048](#)

Resolved Issues: 17.3R2

Authentication, Authorization, and Accounting (AAA) (RADIUS)

- MacSec Issue `show security macsec statistics` command does not show expected results. [PR1283544](#)
- The Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) cannot forward correct Packet Ordering Engine class. [PR1296547](#)
- An l2ald crash occurs with no apparent trigger. [PR1302344](#)
- The CLI command `show snmp mib walk` used for `jnxMIMstMstiPortState` does not display anything in Junos OS Release 17.1R2 on the EX4600 platform. [PR1305281](#)
- Traffic loss is observed while performing NSSU. [PR1311977](#)
- Dhcp-security binding table might not get updated. [PR1312670](#)
- A memory leak is seen for dot1xd. [PR1313578](#)
- The dot1x process might stop authenticating if continuous dot1x clients reauthentication requests can't get processed [PR1300050](#)
- EX series switches do not send radius request after modifying the interface-range configuration. [PR1326442](#)
- QFX5100/EX4600/ACX5k : Major Alarm 'Fan & PSU Airflow direction mismatch' by removing management cable. [PR1327561](#)

Class of Service (CoS)

- On EX4300, EX4600, or QFX5100, traffic might be dropped when there is more than one forwarding class under "forwarding-class-sets". [PR1255077](#)

EVPNs

- Split Horizon Label is not allocated after switching configuration of ESI from 'single-active' to 'all-active' [PR1307056](#)

Infrastructure

- On EX Series switches, the file system might get corrupted multiple times during an image upgrade or commit operation. As a result, the image might fail to upgrade because the EX Series switches bypass the file system corruption check when file system is corrupted. [PR1317250](#)
- On EX4600, priority-based flow control (PFC) frames might not work. [PR1322439](#)

Interfaces and Chassis

- In a Virtual Chassis setup with aggregated Ethernet interfaces and multiple protocols configured in the system, intermittently we see LACP flap when the master is rebooted. Workaround is to toggle the interfaces where LACP is flapping. [PR1301338](#)
- The interface might not work properly after FPC restarts. [PR1329896](#)

Layer 2 Features

- Feature swap-swap might not work as expected in a Q-in-Q scenario. [PR1297772](#)

MPLS

- QFX5100: ISSU is not supported with MPLS configuration. [PR1264786](#)

Platform and Infrastructure

- On EX4300 Virtual Chassis, a 10-Gigabit Ethernet VCP might not get a neighbor after a system reboot. [PR1261363](#)
- CPU utilization for pfex_junos usage might go high if DHCP relay packets are coming continually. [PR1276995](#)
- Traffic loss might be observed for about 10 seconds if master member FPC reboots [PR1283702](#)
- On EX4300 switches, filter-based forwarding (FBF) might not work properly after deactivating or activating. This occurs because stale entries cannot be freed in ternary content addressable memory (TCAM); it leads to insufficient space in TCAM to process filters. [PR1293581](#)
- On an EX4300 switch, packets larger than 1452 bytes will be dropped after generic routing encapsulation (GRE), because the "Fragmentation of payload" and "GRE Path MTU discovery" are not supported on an EX4300 Series switch. [PR1293787](#)
- On EX4300 some functions of IPv6 Router Advertisement Guard do not work. [PR1294260](#)

- **ERROR: /dev/da0s1a is not a JUNOS snapshot** is seen during system startup. [PR1297888](#)
- On EX4300 switches, when unknown unicast ICMP packets are received by an interface, packets are routed, so TTL is decremented. [PR1302070](#)
- On EX4300 Virtual Chassis, the FRU PSU removal and insertion traps are not generated for master or backup FPCs. [PR1302729](#)
- There is an inconsistent IEEE P-bit marking in the 802.1Q header for OSPF packets. [PR1306750](#)
- Traceroute not working in EX9200 device for routing-instances running on 17.1R3 Junos version. [PR1310615](#)
- IGMP snooping might not learn the multicast router interface dynamically. [PR1312128](#)
- On EX4300VC, l2cpd core file might be seen, if the interface is disabled under VSTP and enabled under RSTP [PR1317908](#)
- High latency might be observed between the master Routing Engine and another Flexible PIC Concentrator (FPC). [PR1319795](#)
- On EX4300VC, VSTP BPDUs are not getting processed and root-bridge convergence fails for certain vlans [PR1320719](#)
- Multicast traffic might not get forwarded to one of the receivers. [PR1323499](#)
- A Layer 2 Control Protocol process (l2cpd) might generate a core file. [PR1325917](#)

Routing Protocols

- JDI-RCT:M/Mx:Observed mcsnoopd core @
__raise,abort,__task_quit__,task_quit,task_terminate_timer_callback,task_timer_dispatch,task_scheduler_internal
(enable_slip_detector=true,no_exit=true) at ../../../../src/junos/lib/libjtask/base/task_scheduler.c:275
[.PR1305239](#)

Virtual Chassis

- On EX4300 FRU removal/insertion trap not generated for non-master (backup/line card) FPCs.
[PR1293820](#)

Resolved Issues: 17.3R1

Authentication, Authorization, and Accounting (AAA) (RADIUS)

- VLAN association is not being updated in the Ethernet switching table when the device is configured in single supplicant mode. [PR1283880](#)

Infrastructure

- EX4300 aggregated interface is down while interface member VLAN is PVLAN and LACP is enabled.
[PR1264268](#)

Interfaces and Chassis

- Junos: EX Series PFE and MX MPC7E/8E/9E PFE crash when fetching interface stats with extended-statistics enabled (CVE-2017-10611); Refer to <https://kb.juniper.net/JSA10814> for more information. [PR1247026](#)

Layer 2 Features

- All the XML duplications and unformatted output are addressed. For Example, histogram was just declared as a element inside pfkey container, with this change a new container is defined for histogram. [PR1271648](#)

Platform and Infrastructure

- Layer 3 protocol packets are not being sent out from the switch. [PR1226976](#)

SEE ALSO

New and Changed Features 23
Changes in Behavior and Syntax 31
Known Behavior 35
Known Issues 36
Documentation Updates 46

[Migration, Upgrade, and Downgrade Instructions | 47](#)[Product Compatibility | 48](#)

Documentation Updates

IN THIS SECTION

- [Traffic Management User Guide for EX4600 Switches | 46](#)

This section lists the errata and changes in Junos OS Release 17.3R3 for the EX Series switches documentation.

Traffic Management User Guide for EX4600 Switches

- **Consolidation of the Traffic Management User Guide for QFX Series and EX4600 Switches (EX4600)**—Starting in Junos OS Release 17.3R1, the following three traffic management guides are consolidated into one user guide:
 - Traffic Management User Guide for QFX Series
 - Traffic Management User Guide for QFX 10000 Series
 - Traffic Management User Guide for EX4600 Switches[See [Traffic Management User Guide for QFX Series and EX4600 Switches](#).]
- **Support for deletion of static routes when the BFD session goes down (QFX Series)**—Starting with Junos OS Release 17.3R1, the default behavior of the static route at the **[edit routing-options static static-route bfd-admin-down]** hierarchy level is active. So, the static routes are deleted when the BFD receives a session down message. [See [Enabling BFD on Qualified Next Hops in Static Routes for Route Selection](#).]

SEE ALSO

[New and Changed Features | 23](#)[Changes in Behavior and Syntax | 31](#)[Known Behavior | 35](#)

[Known Issues | 36](#)

[Resolved Issues | 39](#)

[Migration, Upgrade, and Downgrade Instructions | 47](#)

[Product Compatibility | 48](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 47](#)

This section contains the upgrade and downgrade support policy for Junos OS for the EX Series. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network. For information about software installation and upgrade, see the [Installation and Upgrade Guide](#).

Upgrade and Downgrade Support Policy for Junos OS Releases

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 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL 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 on EEOL releases and to review a list of EEOL releases, see <https://support.juniper.net/support/eol/software/junos/>

SEE ALSO

New and Changed Features	23
Changes in Behavior and Syntax	31
Known Behavior	35
Known Issues	36
Resolved Issues	39
Documentation Updates	46
Product Compatibility	48

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 48

Hardware Compatibility

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.

To determine the features supported on EX Series switches in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://pathfinder.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

New and Changed Features	23
Changes in Behavior and Syntax	31
Known Behavior	35
Known Issues	36

[Resolved Issues | 39](#)

[Documentation Updates | 46](#)

[Migration, Upgrade, and Downgrade Instructions | 47](#)

Junos OS Release Notes for Junos Fusion Data Center

IN THIS SECTION

- [New and Changed Features | 49](#)
- [Changes in Behavior and Syntax | 50](#)
- [Known Behavior | 50](#)
- [Known Issues | 51](#)
- [Resolved Issues | 52](#)
- [Documentation Updates | 53](#)
- [Migration, Upgrade, and Downgrade Instructions | 53](#)
- [Product Compatibility | 69](#)

These release notes accompany Junos OS Release 17.3R3 for the Junos Fusion Data Center. 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.

New and Changed Features

There are no new features in Junos OS Release 17.3R3 for Junos Fusion Data Center.

SEE ALSO

[Changes in Behavior and Syntax | 50](#)

[Known Behavior | 50](#)

Known Issues	 51
Resolved Issues	 52
Documentation Updates	 53
Migration, Upgrade, and Downgrade Instructions	 53
Product Compatibility	 69

Changes in Behavior and Syntax

There are no changes in behavior and syntax for Junos Fusion Data Center in Junos OS Release 17.3R3.

SEE ALSO

New and Changed Features	 49
Known Behavior	 50
Known Issues	 51
Resolved Issues	 52
Documentation Updates	 53
Migration, Upgrade, and Downgrade Instructions	 53
Product Compatibility	 69

Known Behavior

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 17.3R3 for Junos Fusion Data Center.

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

Junos Fusion Data Center

- When a QFX10002 switch functions as an aggregation device in a Junos Fusion Data Center topology, it only supports cascade port-based slot assignments for satellite devices. In addition, any change in the configuration for a cascade port connected to a satellite device is treated as a catastrophic event and results in the deletion of any related interface state (including the extended ports), which is rebuilt after a period of time. The following additional restrictions also apply:

- You cannot configure dual-homed satellite device extended ports as pure Layer 3 interfaces. As a result, **family inet** and **family inet6** are not supported on dual-homed extended ports.
- If the ICL interface goes down, traffic loss will occur. As a workaround, we recommend you configure the ICL interface over an aggregated Ethernet interface with multiple links in the bundle to prevent single-point failures that would cause the ICL interface to shut down.

SEE ALSO

New and Changed Features 49
Changes in Behavior and Syntax 50
Known Issues 51
Resolved Issues 52
Documentation Updates 53
Migration, Upgrade, and Downgrade Instructions 53
Product Compatibility 69

Known Issues

There are no known issues in hardware and software in Junos OS Release 17.3R3 for the Junos Fusion Data Center.

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

SEE ALSO

New and Changed Features 49
Changes in Behavior and Syntax 50
Known Behavior 50
Resolved Issues 52
Documentation Updates 53
Migration, Upgrade, and Downgrade Instructions 53
Product Compatibility 69

Resolved Issues

IN THIS SECTION

- [Resolved Issues: Release 17.3R3 | 52](#)
- [Resolved Issues: Release 17.3R2 | 52](#)

This section lists the issues fixed in the Junos main release and maintenance releases.

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

Resolved Issues: Release 17.3R3

Junos Fusion Data Center

- In a fusion setup, an aggregate device may show 'plus' sign on the ICL link for a satellite device. [PR1335373](#)

Resolved Issues: Release 17.3R2

Junos Fusion Data Center

- Native VLAN on an aggregated Ethernet interface terminated on multiple satellite devices. [PR1305698](#)
- In a Junos Fusion topology with LAG on extended ports from satellite devices which are dual-homed to aggregation devices, the LAG interface might flap if rebooting one of the aggregation devices. [PR1315879](#)
- On a Junos Fusion topology with the QFX10002 platform as Aggregate Devices and the Aggregate Devices have dual cascade links to each Satellite Devices as redundancy, duplicated multicast traffic might be seen on downstream devices and multicast receivers if the multicast traffic pass through the Aggregate Devices. As a workaround, please deactivate and re-activate the VLAN in which duplicated multicast traffic is seen. [PR1316499](#)

SEE ALSO

New and Changed Features 49
Changes in Behavior and Syntax 50
Known Behavior 50

[Known Issues | 51](#)

[Documentation Updates | 53](#)

[Migration, Upgrade, and Downgrade Instructions | 53](#)

[Product Compatibility | 69](#)

Documentation Updates

This section lists the errata or changes in Junos OS Release 17.3R3 for Junos Fusion Data Center documentation.

- There are no errata and changes in the current Junos Fusion Data Center documentation.

SEE ALSO

[New and Changed Features | 49](#)

[Changes in Behavior and Syntax | 50](#)

[Known Behavior | 50](#)

[Known Issues | 51](#)

[Resolved Issues | 52](#)

[Migration, Upgrade, and Downgrade Instructions | 53](#)

[Product Compatibility | 69](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading an Aggregation Device | 54](#)
- [Preparing the Switch for Satellite Device Conversion | 56](#)
- [Autoconverting a Switch into a Satellite Device | 58](#)
- [Manually Converting a Switch into a Satellite Device | 61](#)
- [Configuring a Switch into a Satellite Device Before Connecting It to a Junos Fusion Topology | 63](#)
- [Configuring Satellite Device Upgrade Groups | 64](#)
- [Converting a Satellite Device to a Standalone Device | 66](#)

- Upgrade and Downgrade Support Policy for Junos OS Releases | 68
- Downgrading from Release 17.3 | 68

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for Junos Fusion Data Center. Upgrading or downgrading Junos OS can 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 **bundle** 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 [Junos OS Administration Library](#).

The download and installation process for Junos OS Release 17.3R1 is different from previous Junos OS releases.

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:
<https://support.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 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 command, replacing *n* with the spin number.

```
user@host> request system software add reboot
source/jinstall-host-qfx-10-f-17.3R2.n-secure-signed.tgz
```

All other customers, use the following command, replacing *n* with the spin number.

```
user@host> request system software add reboot source/jinstall-host-qfx-10-f-17.3R2
.n-secure-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 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 can take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

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 conversion software requirements, please refer to the [Junos Fusion Hardware and Software Compatibility Matrices](#).

NOTE: For EX4300 switches running Junos OS Release 17.2R1 or QFX5100 switches running Junos OS Release 14.1X53-D43, the following conditions must be met before the Junos switch can be converted to a satellite device when the action is initiated from the aggregation device:

- The Junos switch can only be converted to SNOS 3.1 and higher.
- The Junos switch must be either set to factory-default configuration 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:

```
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 entering 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.

Autoconverting a Switch into a Satellite Device

Use this procedure to automatically configure a switch into a satellite device when it is cabled into the aggregation device.

You can use the autoconversion procedure to add one or more satellite devices to your Junos Fusion topology. The autoconversion procedure is especially useful when you are adding multiple satellite devices to Junos Fusion, because it allows you to easily configure the entire topology before or after cabling the satellite devices to the aggregation devices.

Before you begin:

- Ensure that your aggregation device is running Junos OS Release 17.3R1 or later, and that the satellite devices are running Junos OS Release 14.1X53-D43 or later.

To autoconvert a switch into a satellite device:

1. Cable a link between the aggregation device and the satellite device, if desired.

NOTE: You can cable the aggregation device to the satellite device at any point in this procedure.

When the aggregation device is cabled to the satellite device during this procedure, the process for converting a switch into a satellite device to finalize this process occurs immediately.

If the aggregation device is not cabled to the satellite device, the process for converting a switch into a satellite device to finalize this process starts when the satellite device is cabled to the aggregation device.

2. Log in to the aggregation device.

3. Configure the cascade ports.

For example, to configure interface xe-0/0/1 on the aggregation device into a cascade port:

```
[edit]
user@aggregation-device# set interfaces xe-0/0/1 cascade-port
```

4. Associate an FPC slot ID with each satellite device.

Examples:

- To configure the FPC slot ID of the satellite device that is connected to xe-0/0/1 to 101:

```
[edit]
```

```
user@aggregation-device# set chassis satellite-management fpc 101 cascade-ports xe-0/0/1
```

- To map FPC slot ID 101 to the satellite device using the serial number ABCDEFGHIJKL:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc 101 serial-number
ABCDEFGHIJKL
```

- To map FPC slot ID to the satellite device using MAC address 12:34:56:AB:CD:EF:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc 110 system-id
12:34:56:AB:CD:EF
```

5. (Recommended) Configure an alias name for the satellite device:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc slot-id alias alias-name
```

where *slot-id* is the FPC slot ID of the satellite device defined in the previous step, and *alias-name* is the alias.

For example, to configure the satellite device numbered 101 as qfx5100-48s-1:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc 101 alias qfx5100-48s-1
```

6. Configure an FPC slot ID into a software upgrade group.

For example, to add a satellite device with FPC number 101 to an existing software group named group1, or create a software upgrade group named group1 and add a satellite device with FPC slot 101 to the group:

```
[edit]
user@aggregation-device# set chassis satellite-management upgrade-group group1 satellite
101
```

If you are creating a new software upgrade group in this step, you also need to associate the group with a satellite software image. You can skip this final step if the software upgrade group has been created and an association already exists.

Before associating a satellite software image with a satellite software group, the configuration with the satellite software upgrade group must be committed:

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

After committing the configuration, associate a satellite software image named **satellite-3.1R1.6-signed.tgz** to the upgrade group named **group1**:

```
user@aggregation-device> request system software add /var/tmp/satellite-3.1R1.6-signed.tgz
upgrade-group group1
```

NOTE: Before issuing **request system software add /var/tmp/satellite-3.1R1.6-signed.tgz** **upgrade-group group1**, you must issue a one-time command to expand the storage capacity. Use the **request system storage user-disk expand** command to increase the size of /user partition.

7. Enable automatic satellite conversion:

```
[edit]
user@aggregation-device# set chassis satellite-management auto-satellite-conversion satellite
slot-id
```

For example, to automatically convert FPC 101 into a satellite device:

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

8. Commit the configuration:

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

The satellite software upgrade on the satellite device begins after this final step is completed, or after you cable the satellite device to a cascade port using automatic satellite conversion if you have not already cabled the satellite device to the aggregation device.

After the satellite software update, the switch operates as a satellite device in the Junos Fusion topology

Manually Converting a Switch into a Satellite Device

Use this procedure to manually convert a switch into a satellite device after cabling it into the Junos Fusion topology.

This procedure should be used to convert a switch that is not currently acting as a satellite device into a satellite device. A switch might not be recognized as a satellite device for several reasons, including that the device was not previously autoconverted into a satellite device or that the switch had previously been reverted from a satellite device to a standalone switch.

Before you begin:

- Ensure that your aggregation device is running Junos OS Release 17.3 R1 or later, and that the switches that will become satellite devices are running Junos OS Release 14.1X53-D43 or later.

To manually convert a switch into a satellite device:

1. Cable a link between the aggregation device and the satellite device.
2. Log in to the aggregation device.
3. Configure the link on the aggregation device into a cascade port, if you have not done so already.

For example, to configure interface xe-0/0/1 on the aggregation device into a cascade port:

```
[edit]
user@aggregation-device# set interfaces xe-0/0/1 cascade-port
```

4. Associate an FPC slot ID with the satellite device.

Examples:

- To configure the FPC slot ID of the satellite device that is connected to xe-0/0/1 to 101:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc 101 cascade-ports xe-0/0/1
```

- To map FPC slot ID 101 to the satellite device using the serial number ABCDEFGHIJKL:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc 101 serial-number  
ABCDEFGHIJKL
```

- To map FPC slot ID to the satellite device using MAC address 12:34:56:AB:CD:EF:

```
[edit]
```

```
user@aggregation-device# set chassis satellite-management fpc 110 system-id
12:34:56:AB:CD:EF
```

5. Configure the interface on the aggregation device into a software upgrade group.

For example, to add a satellite device with FPC number 101 to an existing software group named group1, or create a software upgrade group named group1 and add a satellite device configured with FPC number 101 to the group:

```
[edit]
user@aggregation-device# set chassis satellite-management upgrade-group group1 satellite
101
```

If you are creating a new software upgrade group in this step, you also need to associate the group with a satellite software image. You can skip this final step if the software upgrade group has been created and an association already exists.

Before associating a satellite software image with a satellite software group, the configuration with the satellite software upgrade group must be committed:

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

After committing the configuration, associate a satellite software image named **satellite-3.1R1.6-signed.tgz** to the upgrade group named group1:

```
user@aggregation-device> request system software add /var/tmp/satellite-3.1R1.6-signed.tgz
upgrade-group group1
```

NOTE: Before issuing **request system software add /var/tmp/satellite-3.1R1.6-signed.tgz upgrade-group group1**, you must issue a one-time command to expand the storage capacity. Use the **request system storage user-disk expand** command to increase the size of /user partition.

6. Manually configure the switch into a satellite device:

```
user@aggregation-device> request chassis satellite interface interface-name device-mode
satellite
```

For example, to manually configure the switch that is connecting the satellite device to interface xe-0/0/1 on the aggregation device into a satellite device:

```
user@aggregation-device> request chassis satellite interface xe-0/0/1 device-mode satellite
```

The satellite software upgrade on the satellite device begins after this final step is completed.

After the satellite software update, the switch operates as a satellite device in the Junos Fusion topology

Configuring a Switch into a Satellite Device Before Connecting It to a Junos Fusion Topology

Use this procedure to install the satellite software onto a switch before interconnecting it into a Junos Fusion topology as a satellite device. Installing the satellite software on a switch before interconnecting it to a Junos Fusion topology allows you to more immediately deploy the switch as a satellite device by avoiding the downtime associated with the satellite software installation procedure for Junos Fusion.

Before you begin:

- Ensure that your switch that will become a satellite device is running Junos OS Release 14.1X53-D43 or later.
- Ensure that you have copied the satellite software onto the device that will become a satellite device.

NOTE: Ensure there is sufficient space available in the **/var/tmp** directory to be able to copy the software to the switch (especially for EX4300 switches). If there is not enough memory available, issue the **request system storage cleanup** command on the device before attempting to perform the conversion.

In satellite software release 3.1R1, a **satellite-ppc-3.1R1.6-signed.tgz** package is included specifically for converting Junos OS to a satellite device on EX4300 to address a EX4300 switch space issue. The **satellite-ppc** package is to be used only for configuring a switch into a satellite device before connecting it to a Junos Fusion topology.

1. You can manually install the satellite software onto a switch by entering the following command:

```
user@satellite-device> request chassis device-mode satellite URL-to-satellite-software
```

For instance, to install the satellite software package **satellite-3.1R1.6-signed.tgz** stored in the **/var/tmp/** directory on the switch:

```
user@satellite-device> request chassis device-mode satellite  
/var/tmp/satellite-3.1R1.6-signed.tgz
```

- To install satellite software onto a QFX5100 switch, use the **satellite-3.1R1.6-signed.tgz** satellite software package.

- To install satellite software onto a EX4300 switch, use the **satellite-ppc-3.1R1.6-signed.tgz** satellite software package.
2. The device will reboot to complete the satellite software installation.

After the satellite software is installed, follow this procedure to connect the switch into a Junos Fusion topology:

1. Log in to the aggregation device.
2. Configure the link on the aggregation device into a cascade port, if you have not done so already.

For example, to configure interface xe-0/0/1 on the aggregation device into a cascade port:

```
[edit]
user@aggregation-device# set interfaces xe-0/0/1 cascade-port
```

3. Configure the satellite switch into a satellite software upgrade group that is using the same version of satellite software that was manually installed onto the switch.

This step is advisable, but not always required. Completing this step ensures that the satellite software on your device is upgraded to the version of satellite software associated with the satellite software upgrade group when the satellite device connects to the aggregation device.

4. Commit the configuration.

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

5. Cable a link between the aggregation device and the satellite device.

Configuring Satellite Device Upgrade Groups

To simplify the upgrade process for multiple satellite devices, you can create a software upgrade group at the aggregation device, assign satellite devices to the group, and install the satellite software on a groupwide basis.

To create a software upgrade group and assign satellite devices to the group, include the **satellite** statement at the **[edit chassis satellite-management upgrade-groups upgrade-group-name]** hierarchy level.

To configure a software upgrade group and assign satellite devices to the group:

1. Log in to the aggregation device.
2. Create the software upgrade group, and add the satellite devices to the group.

```
[edit]
```



```
user@aggregation-device# set chassis satellite-management upgrade-groups
upgrade-group-name satellite satellite-member-number-or-range
```

upgrade-group-name is the name of the upgrade group, and the **satellite-member-number-or-range** statement is the member numbers of the satellite devices that are being added to the upgrade group. If you enter an existing upgrade group name as the **upgrade-group-name**, you add new satellite devices to the existing software upgrade group.

For example, to create a software upgrade group named group1 that includes all satellite devices numbered 101 through 120, configure the following:

```
[edit]
```

```
user@aggregation-device# set chassis satellite-management upgrade-groups group1 satellite
101-120
```

To install, remove, or roll back a satellite software version on an upgrade group, issue the following operational mode commands:

- **request system software add upgrade-group group-name**—Install the satellite software on all members of the specified upgrade group.
- **request system software delete upgrade-group group-name**—Remove the satellite software association from the specified upgrade group.
- **request system software rollback upgrade-group group-name**—Associate an upgrade group with a previous version of satellite software.

Customers installing satellite software on EX4300 and QFX5100 switches referenced in a software upgrade group, use the following command:

```
user@aggregation-device> request system software add upgrade-group group-name
source/satellite-3.1R1.6-signed.tgz
```

NOTE: Before issuing **request system software add upgrade-group group1**, you must issue a one-time command to expand the storage capacity. Use the **request system storage user-disk expand** command to increase the size of /user partition.

A copy of the satellite software is saved on the aggregation device. When you add a satellite device to an upgrade group that is not running the same satellite software version, the new satellite device is automatically updated to the version of satellite software that is associated with the upgrade group.

You can issue the **show chassis satellite software** command to see which software images are stored on the aggregation device and which upgrade groups are associated with the software images.

Converting a Satellite Device to a Standalone Device

In the event that you need to convert a satellite device to a standalone device, you will need to install a new Junos OS software package on the satellite device and remove it from the Junos Fusion topology.

NOTE: The QFX5100-48SH and QFX5100-48TH satellite device models cannot be converted to a standalone switch.

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 the 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-D43.7-domestic-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://support.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** from the drop-down list and select the switch platform series and model for your satellite device.
4. Select the Junos OS Release 14.1X53D43 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. You can check the automatic satellite conversion configuration by entering the **show** command at the **[edit chassis satellite-management auto-satellite-conversion]** hierarchy level.

```
[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
```

9. Commit the configuration.

```
[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-D43.7-domestic-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-D43.7-domestic-signed.tgz fpc-slot 101
```

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

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

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

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 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL 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://support.juniper.net/support/eol/software/junos/>.

Downgrading from Release 17.3

To downgrade from Release 17.3 to another supported release, follow the procedure for upgrading, but replace the 17.3 **jinstall** package with one that corresponds to the appropriate downgrade release.

NOTE: You cannot downgrade more than three releases.

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

SEE ALSO

New and Changed Features 49
Changes in Behavior and Syntax 50
Known Behavior 50
Known Issues 51
Resolved Issues 52
Documentation Updates 53
Product Compatibility 69

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 69

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guides for the devices used in your Junos Fusion Data Center topology.

To determine the features supported on Junos Fusion devices, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at:
<https://pathfinder.juniper.net/feature-explorer/>

SEE ALSO

New and Changed Features 49
Changes in Behavior and Syntax 50
Known Behavior 50
Known Issues 51
Resolved Issues 52

Documentation Updates | 53

Migration, Upgrade, and Downgrade Instructions | 53

Junos OS Release Notes for Junos Fusion Enterprise

IN THIS SECTION

- [New and Changed Features | 71](#)
- [Changes in Behavior and Syntax | 73](#)
- [Known Behavior | 73](#)
- [Known Issues | 74](#)
- [Resolved Issues | 75](#)
- [Documentation Updates | 77](#)
- [Migration, Upgrade, and Downgrade Instructions | 78](#)
- [Product Compatibility | 86](#)

These release notes accompany Junos OS Release 17.3R3 for Junos Fusion Enterprise. Junos Fusion Enterprise is a Junos Fusion that uses EX9200 switches in the aggregation device role. These release notes describe new and changed features, limitations, and known problems in the hardware and software.

NOTE: For a complete list of all hardware and software requirements for a Junos Fusion Enterprise, including which Juniper Networks devices can function as satellite devices, see [Understanding Junos Fusion Enterprise Software and Hardware Requirements](#).


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.

New and Changed Features

IN THIS SECTION

- [Junos Fusion Enterprise | 72](#)

This section describes the new features and enhancements to existing features in Junos OS Release 17.3R3 for Junos Fusion Enterprise.

**NOTE:** For more information about the Junos Fusion Enterprise features, see the [Junos Fusion Enterprise User Guide](#).

Junos Fusion Enterprise

- **Satellite device support (Junos Fusion Enterprise)**—Starting with Junos OS Release 17.3R1, you can configure QFX5100-48T and QFX5100-48S switches as satellite devices in a Junos Fusion Enterprise topology. The satellite device in a Junos Fusion topology is managed and configured by the aggregation device. Junos Fusion Enterprise uses EX9200 switches in the aggregation device role.
[See [Junos Fusion Enterprise Overview](#).]
- **LAG to single satellite device (Junos Fusion Enterprise)**—Starting in Junos OS Release 17.3R1, you can configure LAGs in a Junos Fusion Enterprise using extended port member links to increase uplink bandwidth and high availability for endpoint devices connected to a satellite device. The member links of the LAG must be on the same satellite device. The LAG can be configured to use LACP, which automates the addition and deletion of individual links to the LAG and can also prevent communication failures by detecting misconfigurations within a LAG.
[See [Configuring Link Aggregation on Satellite Devices in a Junos Fusion Enterprise](#).]

SEE ALSO

Changes in Behavior and Syntax	73
Known Behavior	73
Known Issues	74
Resolved Issues	75
Documentation Updates	77
Migration, Upgrade, and Downgrade Instructions	78
Product Compatibility	86

Changes in Behavior and Syntax

IN THIS SECTION

- [Junos Fusion Enterprise | 73](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 17.3R3 for Junos Fusion Enterprise.

Junos Fusion Enterprise

- For the **request chassis satellite beacon** operational command, the **slot-id** option has been changed to **fpc-slot**. This change was made to support enabling beacon functionality for individual FPCs. [PR1272956](#)

SEE ALSO

New and Changed Features 71
Known Behavior 73
Known Issues 74
Resolved Issues 75
Documentation Updates 77
Migration, Upgrade, and Downgrade Instructions 78
Product Compatibility 86

Known Behavior

IN THIS SECTION

- [Junos Fusion Enterprise | 74](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 17.3R3 for Junos Fusion Enterprise.

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

Junos Fusion Enterprise

- In a Junos Fusion Enterprise topology with dual aggregation devices, firewall statistics are not synced across the aggregation devices. [PR1105612](#)
- In a Junos Fusion Enterprise, the **show ethernet-switching table** command takes a few minutes to show entries when received on an extended port with MAC count set to 150K. [PR1117567](#)
- In a Junos Fusion Enterprise, to use a non-default port as a clustering port in a clustering port policy, the policy must include at least one port that is a default uplink/clustering port for that platform. [PR1241808](#)
- In a Junos Fusion Enterprise, the satellite device link goes down with autonegotiation enabled when the link partner speed is 100 Mbps. [PR1272107](#)
- In a Junos Fusion Enterprise, Auto_MDIX and EEE are not supported on the QFX5100 as a satellite device. The configuration commit succeeds on **ge-** ports but the features are not enabled. [PR1279928](#)

SEE ALSO

New and Changed Features 71
Changes in Behavior and Syntax 73
Known Issues 74
Resolved Issues 75
Documentation Updates 77
Migration, Upgrade, and Downgrade Instructions 78
Product Compatibility 86

Known Issues

IN THIS SECTION

- [Junos Fusion Enterprise | 75](#)

This section lists the known issues in hardware and software in Junos OS Release 17.3R3 for Junos Fusion Enterprise.

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

Junos Fusion Enterprise

- On a Junos Fusion, when using LLDP, the "Power via MDI" and "Extended Power via MDI" TLVs are not transmitted. [PR1105217](#)
- On a Junos Fusion, the `tcpdump` command does not capture packets on satellite devices. [PR1125568](#)
- On a Junos Fusion Enterprise, Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) fast start does not work. [PR1171899](#)
- On a Junos Fusion Enterprise, when the satellite devices of a cluster are rebooted, the output of the CLI command `show chassis satellite` shows the port state of the cascade ports as "Present". [PR1175834](#)

SEE ALSO

New and Changed Features 71
Changes in Behavior and Syntax 73
Known Behavior 73
Resolved Issues 75
Documentation Updates 77
Migration, Upgrade, and Downgrade Instructions 78
Product Compatibility 86

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 17.3R3 | 76](#)
- [Resolved Issues: 17.3R2 | 76](#)
- [Resolved Issues: 17.3R1 | 77](#)

This section lists the issues fixed in the Junos OS main release and the maintenance releases for Junos Fusion 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: 17.3R3

Junos Fusion Enterprise

- Mirrored packets are dropped if analyzer output extended port is reachable through the ICL link. [PR1211123](#)
- In a Junos Fusion environment, the satellite device displays U-boot on the LCD screen. [PR1304784](#)
- Packet loss of 2-3 seconds is seen every 5 minutes on a Junos Fusion. [PR1320254](#)
- An scpd core file might be seen on an aggregation device when a dynamic ACL on an 802.1X-enabled port is installed on a single-homed satellite device. [PR1328247](#)
- DHCP security binding entries are not synced after the FPC goes offline and then online. [PR1332828](#)
- This PR is an 802.1X re-authentication issue. [PR1345365](#)

Resolved Issues: 17.3R2

Junos Fusion Enterprise

- While applying a loopback filter on aggregation devices in a Junos Fusion Enterprise, Callback Control Protocol (CBCP) packets might be filtered, which might cause CBCP sessions to be dropped and one of the satellite devices in a redundant pair to be in the SplitBrainDn state. [PR1183680](#)
- Request chassis satellite beacon functionality to specific satellite device (SD) is not working, causing all the SDs to enable the beacon LED. [PR1272956](#)
- VRRP has a split brain in a dual autodiscovery Junos Fusion. [PR1293030](#)
- On a dual aggregation device Fusion setup, PoE is not working on one of the satellite devices in a satellite cluster. [PR1295556](#)
- On a Junos Fusion Enterprise with dual aggregation devices (ADs), if you apply Routing Engine loopback filters and bring down the cascade port on one of the ADs, the satellite device (SD) on the AD where the cascade port is down goes to ProvSessDown due to a TCP session drop over the ICL interface. As a workaround, add additional filters to bypass the ICL traffic for the ICL interface's IP address. [PR1275290](#)
- An aggregation device without a cascade port cannot reach hosts over an ICL link if they are authenticated by 802.1X in a different VLAN than the default (manually assigned) VLAN. [PR1298880](#)
- The 802.1X authentication fails on a Junos Fusion setup. [PR1299532](#)

- The 802.1X authentication might crash in a Junos Fusion setup with dual aggregation devices. [PR1303909](#)
- All the 802.1X authentication sessions are removed when the auto-ICCP link is disabled. [PR1307588](#)
- LACP aggregated Ethernet interfaces go to a **DOWN** state when performing **commit synchronize**. [PR 1314561](#)

Resolved Issues: 17.3R1

Junos Fusion Enterprise

- On a Junos Fusion Enterprise, an upgrade group's association with a satellite software version is removed if the chassis satellite-management redundancy-groups configuration is deleted. [PR1267370](#)
- On a Junos Fusion Enterprise, traffic shaping is not supported on the extended ports. [PR1268084](#)
- When a race condition results in a dynamic VLAN assignment, the MAC-based VLAN (MBV) entry might not get created on the peer aggregation device. This situation can result in traffic loss when it flows through the peer AD. [PR1282828](#)

SEE ALSO

New and Changed Features 71
Changes in Behavior and Syntax 73
Known Behavior 73
Known Issues 74
Documentation Updates 77
Migration, Upgrade, and Downgrade Instructions 78
Product Compatibility 86

Documentation Updates

There are no errata or changes in Junos OS Release 17.3R3 for Junos Fusion Enterprise documentation.

SEE ALSO

New and Changed Features 71
Changes in Behavior and Syntax 73
Known Behavior 73

[Known Issues | 74](#)

[Resolved Issues | 75](#)

[Migration, Upgrade, and Downgrade Instructions | 78](#)

[Product Compatibility | 86](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading Junos OS on an Aggregation Device | 78](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 81](#)
- [Preparing the Switch for Satellite Device Conversion | 81](#)
- [Converting a Satellite Device to a Standalone Switch | 82](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 85](#)
- [Downgrading from Release 17.3 | 85](#)

This section contains the procedure to upgrade or downgrade Junos OS and satellite software for a Junos Fusion Enterprise. Upgrading or downgrading Junos OS and satellite software might take several hours, depending on the size and configuration of the Junos Fusion 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 Release 17.3R1:

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:
<https://support.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, replacing *n* with the spin number.

```
user@host> request system software add validate reboot  
source/junos-install-ex92xx-x86-64-17.3R1.n.tgz
```

All other customers, use the following commands, replacing *n* with the spin number.

```
user@host> request system software add validate reboot  
source/junos-install-ex92xx-x86-64-17.3R1.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.

NOTE: To upgrade from Junos OS 17.1 to 17.3R1, use the procedure for upgrading from Junos OS 17.1 to 17.2, as documented in the Release Notes for Junos Fusion Enterprise, Junos OS Release 17.2.

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 Enterprise. See [Configuring or Expanding a Junos Fusion Enterprise](#).

For satellite device hardware and software requirements, see [Understanding Junos Fusion 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: For EX4300 switches running Junos OS Release 17.2R1, QFX5100 switches running Junos OS Release 14.1X53-D43 or EX2300 and EX3400 switches running Junos OS Release 15.1X53-D55.5, the following conditions must be met before the Junos switch can be converted to a satellite device when the action is initiated from the aggregation device:

- The Junos switch can only be converted to SNOS 3.1 and higher.
- The Junos switch must be either set to factory-default configuration 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:

```
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. (EX3400 and 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 EX3400 and 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 Enterprise](#) for detailed configuration steps for each method.

Converting a Satellite Device to a Standalone Switch

In the event that you need to convert a satellite device to a standalone device, you will need to install a new Junos OS software package on the satellite device and remove the satellite device from the Junos Fusion topology.

The following steps explain how to convert a satellite device that is participating in a Junos Fusion to a standalone device running Junos OS. If you have a standalone switch that is not part of a Junos Fusion but is running satellite software, and you want the switch to run Junos OS software, see [Installing Junos OS Software on a Standalone Device Running Satellite Software](#).

NOTE: Conversion of EX2300 and EX3400 switches from satellite devices to standalone devices cannot be initiated from the aggregation device. To install Junos OS software on an EX2300 or EX3400 switch acting as a satellite device, see [Installing Junos OS Software on a Standalone Device Running Satellite Software](#).

The following steps explain how to download software, remove the satellite device from the 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://support.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** from the menu and select the switch platform series and model for your satellite device.
4. Select the software image for your platform, using the following guidelines:
 - If the satellite device is a EX4300 switch, you install a standard, signed **jinstall** version of Junos OS.
 - If the satellite device is a QFX5100 switch that can be converted to a standalone device, you must install a Preboot eXecution Environment (PXE) version of Junos OS. The PXE version of Junos OS software supports the same feature set as the other Junos OS software packages for a release, but is specially engineered to install Junos OS onto a device running satellite software. The PXE Junos OS package name uses the format **install-media-pxe-qfx-5-version-domestic-signed.tgz**.
5. Review and accept the End User License Agreement.
6. Download the software to a local host.
Copy the software to the routing platform or to your internal software distribution site.
7. 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 the 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.

8. Commit the configuration.

To commit the configuration to both Routing Engines:

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

To commit the configuration to a single Routing Engine:

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

9. Install Junos OS 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 software package stored in the **/var/tmp** directory on the aggregation device onto a switch acting as the satellite device using FPC slot 102:

```
[edit]
user@aggregation-device> request chassis satellite install /var/tmp/package-name fpc-slot 102
```

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

10. Wait for the reboot that accompanies the software installation to complete.
11. When you are prompted to log back in to your device, uncable the device from the Junos Fusion topology. See *Remove a Transceiver*. Your device is removed from the Junos Fusion.

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

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 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL 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 on EEOL releases and to review a list of EEOL releases, see <https://support.juniper.net/support/eol/software/junos/>

Downgrading from Release 17.3

Junos Fusion 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.

To downgrade a Junos Fusion Enterprise, follow the procedure for upgrading, but replace the 17.2 **junos-install** package with one that corresponds to the appropriate release.

NOTE: We recommend that you do not downgrade the aggregation device from 17.3R1 to 17.2 if there are cluster satellite devices in the setup.

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

SEE ALSO

New and Changed Features 71
Changes in Behavior and Syntax 73
Known Behavior 73
Known Issues 74
Resolved Issues 75
Documentation Updates 77
Product Compatibility 86

Product Compatibility

IN THIS SECTION

- [Hardware and Software Compatibility | 86](#)
- [Hardware Compatibility Tool | 87](#)

Hardware and Software Compatibility

For a complete list of all hardware and software requirements for a Junos Fusion Enterprise, including which Juniper Networks devices function as satellite devices, see [Understanding Junos Fusion Enterprise Software and Hardware Requirements](#) in the [Junos Fusion Enterprise User Guide](#).

To determine the features supported on Junos Fusion devices, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at: <https://pathfinder.juniper.net/feature-explorer/>

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

New and Changed Features 71
Changes in Behavior and Syntax 73
Known Behavior 73
Known Issues 74
Resolved Issues 75
Documentation Updates 77
Migration, Upgrade, and Downgrade Instructions 78

Junos OS Release Notes for Junos Fusion Provider Edge

IN THIS SECTION

- New and Changed Features | 88
- Changes in Behavior and Syntax | 90
- Known Behavior | 90
- Known Issues | 91
- Resolved Issues | 92
- Documentation Updates | 93
- Migration, Upgrade, and Downgrade Instructions | 94
- Product Compatibility | 102

These release notes accompany Junos OS Release 17.3R3 for the Junos Fusion 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.

New and Changed Features

IN THIS SECTION

- Release 17.3R3 New and Changed Features | 89
- Release 17.3R2 New and Changed Features | 89
- Release 17.3R1 New and Changed Features | 89

This section describes the new features and enhancements to existing features in the Junos OS main release and the maintenance releases for Junos Fusion Provider Edge.

Release 17.3R3 New and Changed Features

There are no new features or enhancements to existing features for Junos Fusion Provider Edge in Junos OS Release 17.3R3.

Release 17.3R2 New and Changed Features

There are no new features or enhancements to existing features for Junos Fusion Provider Edge in Junos OS Release 17.3R2.

Release 17.3R1 New and Changed Features

Junos Fusion

- **Power over Ethernet (PoE) for Junos Fusion Provider Edge**—Starting in Junos OS Release 17.3R1, PoE is supported on Junos Fusion Provider Edge. PoE enables electric power, along with data, to be passed over a copper Ethernet LAN cable. Powered devices—such as VoIP telephones, wireless access points, video cameras, and point-of-sale devices—that support PoE can receive power safely from the same access ports that are used to connect personal computers to the network. This reduces the amount of wiring in a network, and also eliminates the need to position a powered device near an AC power outlet, making network design more flexible and efficient.

In a Junos Fusion system, PoE is used to carry electric power from an extended port on a satellite device to a connected device. An extended port is any network-facing port on a satellite device in a Junos Fusion Provider Edge. All extended ports that support PoE on satellite devices in a Junos Fusion Provider Edge support the IEEE 802.3at PoE+ standard. The aggregation device on Junos Fusion Provider Edge manages PoE support of PoE-capable interfaces on satellite device. Junos Fusion Provider Edge only supports PoE with EX series switches as satellite devices and an MX Series 5G Universal Routing Platform as the aggregation device.

[See [Understanding Power over Ethernet in a Junos Fusion](#).]

- **Port-based network access control**—Starting in Junos OS Release 17.3R1, Junos Fusion Provide Edge supports port-based authentication as defined by the IEEE 802.1X standard and central Web authentication to prevent unauthorized network access on extended ports of the satellite devices. This feature allows you to configure satellite devices to block access to the network until the client is authenticated. This feature allows you to configure satellite devices to block access to the network until the client is authenticated.

[See [Understanding port-based authentication in a Junos Fusion Provider Edge](#).]

- **Metro Ethernet Forum (MEF) Carrier Ethernet 2.0 Certification**—Starting in Junos OS Release 17.3R1, Junos Fusion Provider Edge qualifies for Carrier Ethernet 2.0 (CE2.0) certification. This ensures that the

routers and switches in a Junos Fusion Provider Edge system comply withto the Carrier Ethernet specification set by the MEF.

SEE ALSO

Changes in Behavior and Syntax 90
Known Behavior 90
Known Issues 91
Resolved Issues 92
Documentation Updates 93
Migration, Upgrade, and Downgrade Instructions 94
Product Compatibility 102

Changes in Behavior and Syntax

There are no changes in default behavior and syntax for Junos Fusion Provider Edge in Junos OS Release 17.3R3.

SEE ALSO

New and Changed Features 88
Known Behavior 90
Known Issues 91
Resolved Issues 92
Documentation Updates 93
Migration, Upgrade, and Downgrade Instructions 94
Product Compatibility 102

Known Behavior

There are no known behaviors, system maximums, and limitations in hardware and software for Junos Fusion Provider Edge in Junos OS Release 17.3R3.

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

SEE ALSO

New and Changed Features	 88
Changes in Behavior and Syntax	 90
Known Issues	 91
Resolved Issues	 92
Documentation Updates	 93
Migration, Upgrade, and Downgrade Instructions	 94
Product Compatibility	 102

Known Issues

There are no known issues in the Junos OS Release 17.3R3 for Junos Fusion Provider Edge.

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

SEE ALSO

New and Changed Features	 88
Changes in Behavior and Syntax	 90
Known Behavior	 90
Resolved Issues	 92
Documentation Updates	 93
Migration, Upgrade, and Downgrade Instructions	 94
Product Compatibility	 102

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 17.3R3 | 92](#)
- [Resolved Issues: 17.3R2 | 92](#)
- [Resolved Issues: 17.3R1 | 93](#)

This section lists the issues fixed in the Junos OS main release and the maintenance releases.

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

Resolved Issues: 17.3R3

Junos Fusion Provider Edge

- Some VLAN bridges and VTEP bindings might be lost after deleting or deactivating a VLAN and then committing configuration. [PR1298659](#)
- Duplicated packets might be received on the multicast downstream devices and multicast receivers. [PR1316499](#)
- In Junos fusion **show interfaces diagnostics optics satellite** command does not display any outputs. [PR1327876](#)
- The aggregate device might show 'plus' sign on the ICL link for a satellite device. [PR1335373](#)
- High IGMP leave latency with igmp snooping in EVPN. [PR1327980](#)
- SSH key-based authentication fails after reboot if **chassis satellite-management** is configured. [PR1344392](#)

Resolved Issues: 17.3R2

Junos Fusion Provider Edge

- Some vlan bridges and VTEP bindings might be lost after deleting or deactivating a vlan and then committing configuration. [PR1298659](#)
- The LAG interface might flap if rebooting aggregation device. [PR1315879](#)
- Duplicated packets might be received on the multicast downstream devices and multicast receivers. [PR1316499](#)

Junos Fusion Satellite Software

- Native VLAN on an aggregated Ethernet interface terminated on multiple satellite devices. [PR1305698](#)

Resolved Issues: 17.3R1

There are no fixed issues in the Junos OS Release 17.3R1 for Junos Fusion Provider Edge.

SEE ALSO

New and Changed Features 88
Changes in Behavior and Syntax 90
Known Behavior 90
Known Issues 91
Documentation Updates 93
Migration, Upgrade, and Downgrade Instructions 94
Product Compatibility 102

Documentation Updates

There are no errata or changes in Junos OS Release 17.3R3 for Junos Fusion Provider Edge documentation.

SEE ALSO

New and Changed Features 88
Changes in Behavior and Syntax 90
Known Behavior 90
Known Issues 91
Resolved Issues 92
Migration, Upgrade, and Downgrade Instructions 94
Product Compatibility 102

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Basic Procedure for Upgrading an Aggregation Device | 94
- Upgrading an Aggregation Device with Redundant Routing Engines | 96
- Preparing the Switch for Satellite Device Conversion | 97
- Converting a Satellite Device to a Standalone Device | 98
- Upgrading an Aggregation Device | 100
- Upgrade and Downgrade Support Policy for Junos OS Releases | 101
- Downgrading from Release 17.3 | 101

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for Junos Fusion 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 [Junos OS Administration Library](#).

The download and installation process for Junos OS Release 17.3R3 is different that for earlier Junos OS releases.

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

NOTE: We highly recommend that you see 64-bit Junos OS software when implementing Junos Fusion Provider Edge.

For upgrades from Junos Release 14.2 and earlier:

```
user@host> request system software add no-validate reboot source/package-name
```

All other upgrades:

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

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 17.3R3 **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: For EX4300 switches running Junos OS Release 17.2R1 or QFX5100 switches running Junos OS Release 14.1X53-D43, the following conditions must be met before a Junos switch can be converted to a satellite device when the action is initiated from the aggregation device:

- The Junos switch can only be converted to SNOS 3.1 and higher.
- The Junos switch must be either set to factory-default configuration 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 validate 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 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:

```
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 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 Provider Edge](#) for detailed configuration steps for each method.

Converting a Satellite Device to a Standalone Device

In the event that you need to convert a satellite device to a standalone device, you will need to 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://support.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** 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-D43 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 once the software installation starts. The software upgrade starts after this command is entered.

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

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

Upgrading an Aggregation Device

When you upgrade an aggregation device to Junos OS Release 17.3R3, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

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 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL 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://support.juniper.net/support/eol/software/junos/>.

Downgrading from Release 17.3

To downgrade from Release 17.3 to another supported release, follow the procedure for upgrading, but replace the 17.3 **jinstall** package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

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

SEE ALSO

[New and Changed Features | 88](#)

[Changes in Behavior and Syntax | 90](#)

[Known Behavior | 90](#)

[Known Issues | 91](#)

[Resolved Issues | 92](#)

[Documentation Updates | 93](#)

[Product Compatibility | 102](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 102](#)

Hardware Compatibility

Hardware Compatibility

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

To determine the features supported on MX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. See the [Feature Explorer](#).

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

New and Changed Features 88
Changes in Behavior and Syntax 90
Known Behavior 90
Known Issues 91
Resolved Issues 92
Documentation Updates 93
Migration, Upgrade, and Downgrade Instructions 94

Junos OS Release Notes for MX Series 5G Universal Routing Platforms

IN THIS SECTION

- New and Changed Features | 103
- Changes in Behavior and Syntax | 135
- Known Behavior | 145
- Known Issues | 154
- Resolved Issues | 174
- Documentation Updates | 214
- Migration, Upgrade, and Downgrade Instructions | 215
- Product Compatibility | 222

These release notes accompany Junos OS Release 17.3R3 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

NOTE: Unified in-service software upgrade (ISSU) is not recommended on MX Series platforms to upgrade from previous Junos OS releases to Junos OS 17.3R3. For more information, see [“Known Issues” on page 154](#).

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.

New and Changed Features

IN THIS SECTION

- Release 17.3R3-S12 New and Changed Features | 105
- Release 17.3R3 New and Changed Features | 105

- [Release 17.3R2 New and Changed Features | 110](#)
- [Release 17.3R1 New and Changed Features | 110](#)

This section describes the new features and enhancements to existing features in the Junos OS main release and the maintenance releases for MX Series.

Release 17.3R3-S12 New and Changed Features

General Routing

- **Displaying accurate aggregate drop statistics (MX Series)**—You can view the accurate aggregate drop statistics when a packet drop is seen on an aggregated Ethernet interface by using the **show interfaces extensive** command. In earlier releases, the **show interfaces extensive** command did not display accurate aggregate drop statistics. Only the individual aggregate child interface displayed accurate drop statistics.

Release 17.3R3 New and Changed Features

Interfaces and Changes

- **Enhancement to increase the threshold of corrected single-bit errors (MPC7E, MPC8E, MPC9E on MX Series)**—In Junos OS Release 17.3R3, the threshold of corrected single-bit error is increased from 32 to 1024, and the alarm severity is changed from Major to Minor for those error messages. There is no operational impact upon corrected single bit errors. Also, a log message is added to display how many single-bit errors have been corrected between the reported events as follows:

EA[0:0]: HMCIF Rx: Link0: Corrected single bit errordetected in HMC 0 - Total count 25

EA[0:0]: HMCIF Rx: Link0: Corrected single bit errordetected in HMC 0 - Total count 26

[See [Alarm Overview](#).]

Restoration Procedures and Failure

- **Device recovery mode introduced in Junos OS with upgraded FreeBSD (MX Series)**—In Junos OS Release 17.3R3, for devices running Junos OS with upgraded FreeBSD, provided you have saved a rescue configuration on the device, there is an automatic device recovery mode that goes into action should the system go into amnesiac mode. The new process is for the system to automatically retry to boot with the saved rescue configuration. In this circumstance, the system displays a banner "Device is in recovery mode" in the CLI (in both the operational and configuration modes). Previously, there was no automatic process to recover from amnesiac mode. A user with load and commit permission had to log in using the console and fix the issue in the configuration before the system would reboot.

[See [Saving a Rescue Configuration File](#).]

Services Applications

- **Support for filtering DNS requests for blacklisted website domains (MX Series with MS-MPCs)**—Starting in Junos OS Release 17.3R3, you can configure DNS filtering to identify DNS requests for blacklisted website domains.

For DNS request types A, AAAA, MX, CNAME, TXT, SRV, and ANY, you also configure the action to take for a DNS request for a blacklisted domain. You can either:

- Block access to the website by sending the client a DNS response corresponding to the DNS request type with the IP address or fully qualified domain name (FQDN) of a DNS sinkhole server. This ensures that the client sends further traffic for the blacklisted domain to the sinkhole server.

- Log the request and allow access.

For other DNS request types for a blacklisted domain, the request is logged and access is allowed.

To configure DNS filtering:

1. Create one or more domain filter database files that include an entry for each blacklisted domain. The database file must have a **.txt** extension. A database file can have a maximum of 10,000 domain entries, and the file name can have a maximum length of 64 characters.

The file header should have a format such as

20170314_01:domain,sinkhole_ip,v6_sinkhole,sinkhole_fqdn,id,action.

Each entry in the database file has the following items:

hashed-domain-name,IPv4 sinkhole address,IPv6 sinkhole address,sinkhole FQDN,ID,action

where:

- **hashed-domain-name** is a hashed value of the blacklisted domain name (64 hexadecimal characters). The hash method and hash key that you use to produce the hashed domain value are needed when you configure DNS filtering with the Junos OS CLI.
- **IPv4 sinkhole address** is the address of the DNS sinkhole server for IPv4 DNS requests.
- **IPv6 sinkhole address** is the address of the DNS sinkhole server for IPv6 DNS requests.
- **sinkhole FQDN** is the fully qualified domain name of the DNS sinkhole server.
- **ID** is a 32-bit number that uniquely associates the entry with the hashed domain name.
- **action** is the action to apply to a DNS request that matches the blacklisted domain name. If you enter **replace**, the MX series router sends the client a DNS response with the IP address or FQDN of the DNS sinkhole server. If you enter **report**, the DNS request is logged and then sent to the DNS server.

The last line of the file should have the file hash, which you calculate using the same key and hash method that you used to produce the hashed domain names.

2. Save the database files on the Routing Engine in the **/var/db/url-filterd**.
3. Configure a DNS filter profile. A DNS filter profile includes general DNS filtering settings and up to 32 templates. Each template identifies an uplink and downlink logical interface on which to apply specific DNS filtering settings. The **dns-filter** settings within a template (**[edit services web-filter profile *profile-name* dns-filter-template *template-name* dns-filter]**) override the corresponding settings at the DNS profile level (**[edit services web-filter profile *profile-name* dns-filter]**).

You can configure up to eight profiles.

```
[edit services]
```

```

web-filter {
  profile profile-name {
    dns-filter {
      database-file filename;
      dns-resp-ttl minutes;
      dns-server [ ip-address ];
      hash-method hash-method-name;
      hash-key key-string;
      statistics-log-timer minutes;
      wildcarding-level level;
    }
    dns-filter-template template-name {
      client-interfaces [ client-interface-name ];
      client-routing-instance client-routing-instance-name;
      dns-filter {
        database-file filename;
        dns-resp-ttl minutes;
        dns-server [ ip-address ];
        hash-key key-string;
        hash-method hash-method-name;
        statistics-log-timer minutes;
        wildcarding-level level;
      }
      server-interfaces [ server-interface-name ];
      server-routing-instance server-routing-instance-name;
      term term-name {
        from {
          src-ip-prefix [ source-prefix ];
        }
        then {
          accept;
          dns-sinkhole;
        }
      }
    }
    global-dns-stats-log-timer minutes
  }
}

```

The following items describe the statements:

- **profile *profile-name***—Specify a name for the DNS filter profile.
- **global-dns-stats-log-timer *minutes***—Specify the interval for logging system-level statistics for DNS filtering. The range is 0 through 60 minutes and the default is 5 minutes.

- **database-file *filename***—Specify the name of the domain filter database to use. The setting within a template overrides the corresponding setting at the DNS profile level.
- **dns-server [*ip-address*]**—(Optional) To limit DNS filtering to DNS requests that are destined for specific DNS servers, specify up to three IP addresses (IPv4 or IPv6). The setting within a template overrides the corresponding setting at the DNS profile level.
- **hash-method *hash-method-name***—Specify the hash method that was used to create the hashed domain name in the domain filter database file. The setting within a template overrides the corresponding setting at the DNS profile level.
- **hash-key *key-string***—Specify the hash key that was used to create the hashed domain name in the domain filter database file. The setting within a template overrides the corresponding setting at the DNS profile level.
- **statistics-log-timer *minutes***—Specify the interval for logging statistics for DNS requests and for sinkhole actions performed for each client and customer IP address. The range is 1 through 60 minutes and the default is 5 minutes. The setting within a template overrides the corresponding setting at the DNS profile level.
- **dns-resp-ttl *minutes***—Specify the time to live while sending the DNS response after taking the DNS sinkhole action. The range is 0 through 86,400 seconds and the default is 1800. The setting within a template overrides the corresponding setting at the DNS profile level.
- **wildcarding-level *level***—Specify the level of subdomains that are searched for a match. The range is 0 through 10. A value of 0 indicates that subdomains are not searched. The setting within a template overrides the corresponding setting at the DNS profile level.
- **dns-filter-template *template-name***—Specify the name of a template.
- **client-interfaces [*client-interface-name*]**—Specify the client-facing logical interfaces (uplink) on which the DNS filtering is configured for the template.
- **server-interfaces [*server-interface-name*]**—Specify the server-facing logical interfaces (downlink) on which the DNS filtering is configured for the template.
- **client-routing-instance *client-routing-instance-name***—Specify the routing instance on which the client-facing logical interface DNS filtering is configured for the template.
- **server-routing-instance *server-routing-instance-name***—Specify the routing instance on which the server-facing logical interface DNS filtering is configured for the template.

NOTE: If you configure the client and server interfaces or the client and server routing instances, implicit filters are installed on the interfaces or routing instances to direct DNS traffic to the MS-MPC for DNS filtering. If you configure neither the client and server interfaces nor the routing instances, you must provide a way to direct DNS traffic to the MS-MPC (for example, via routes).

- **term *term-name***—Configure a term for the template. You can configure a maximum of 64 terms in a template.
 - **src-ip-prefix [*source-prefix*]**—Specify the source IP addresses of DNS requests you want to filter. You can configure a maximum of 64 addresses in a term.
 - **dns-sinkhole**—Specify that the sinkhole action identified in the domain filter database is performed on blacklisted DNS requests that match the **src-ip-prefix**.
4. Associate the DNS filter profile with a next-hop service set and enable logging for DNS filtering. The service interface can be an aggregated multiservices (AMS) interface.

```
[edit services]
service-set service-set-name {
    web-filter-profile profile-name;
    syslog host local class urlf-logs;
    next-hop-service {
        inside-service-interface interface-name.unit-number;
        outside-service-interface interface-name.unit-number;
    }
}
```

To display statistics for the DNS filtering performed by a profile, use the **show services web-filter statistics fpc-slot *fpc-slot* pic-slot *pic-slot* profile *profile-name* dns-filter-template *template-name* dns-filter-term *term-name*** command. The **profile** option is required.

To clear statistics for the DNS filtering, use the **clear services web-filter statistics fpc-slot *fpc-slot* pic-slot *pic-slot* profile *profile-name* dns-filter-template *template-name*** command. The **profile** option is required.

To apply any changes you make to a domain filter database file, use the **request services web-filter update dns-filter-database *filename*** command.

To validate a domain filter database file, use the **request services web-filter validate dns-filter-file-name filename hash-key key-string hash-method hash-method-name** command.

Software Installation and Upgrade

- **ZTP support is added for MX VM host platforms (MX Series)**—In Junos OS Release 17.3R3, ZTP, which automates the provisioning of the device configuration and software image with minimal manual intervention, is supported on MX Series VM hosts. When you physically connect a supported device to the network and boot it with a factory configuration, the device attempts to upgrade the Junos OS software image automatically and autoinstall a configuration provided on the DHCP server.

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

Subscriber Management and Services

- **Controlling search behavior for address allocation from linked pools (MX Series)**—Starting in Junos OS Release 17.3R3, you can use the **linked-pool-aggregation** statement at the **[edit access]** hierarchy level to change how addresses are allocated from linked IP address pools. When you configure the statement, addresses can be assigned from a later pool in the chain before an earlier pool is depleted. When the statement is not configured, IP addresses are assigned contiguously, so that all addresses are allocated from the matching pool and then the first pool in the chain before addresses are assigned from a linked pool.

[See [Configuring Address-Assignment Pool Linking](#).]

VPNs

- **Increased number of supported routing instances instances (MX240, MX480, MX960, MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 17.3R3, Junos OS supports up to 16K VPLS routing instances with 128K (FEC 128) hierarchical VPLS pseudowires.

NOTE: Nonstop active routing (NSR) is not supported for all 16K routing instances.

[See [Configuring VPLS Routing Instances](#).]

Release 17.3R2 New and Changed Features

There are no new features or enhancements to existing features for MX Series routers in Junos OS Release 17.3R2.

Release 17.3R1 New and Changed Features

Class of Service (CoS)

- **Support for efficient use of CoS resources on targeted interfaces (MX Series)**—Starting in Junos OS Release 17.3R1, when you configure Junos OS to target the egress traffic for a subscriber on a single

member link, Junos OS applies CoS resources only to the active link, optimizing the use of available scheduling nodes. If the assigned primary link goes down, CoS scheduling resources are switched to the backup link.

[See [targeted-distribution \(Dynamic Demux Interfaces over Aggregated Ethernet\)](#).]

- **Support for setting the DSCP code point for host-originating IS-IS traffic sent over a GRE tunnel (MX Series)**—Starting in Junos OS Release 17.3R1, you can determine traffic prioritization for IS-IS traffic originating on a host and being sent over a GRE tunnel by assigning a DSCP code point to the IS-IS packets. You can set the DSCP code point by including the `isis-over-gre dscp-code-point value` statement at the `[edit class-of-service host-outbound-traffic protocol]` hierarchy level.

[See [protocol \(Host Outbound Traffic\)](#).]

Dynamic Host Configuration Protocol (DHCP)

- **Support for single-session DHCP dual-stack subscriber for S-VLAN model server and relay (MX Series)**—Starting in Junos OS Release 17.3R1, DHCP dual-stack subscriber for N:1 (IP demux) access models support multiple household share the same S-VLAN.

A dual-stack DHCP subscriber is represented as a single subscriber with a single session database (SDB) session.

The benefits of a single-session dual-stack model are as follows:

- Simplifies router configuration.
- Reduces RADIUS message load.
- Reduces the backend correlation of multiple accounting sessions for the same household.
- Is compatible with existing RADIUS messaging.

[See [Single-Session DHCP Local Server Dual-Stack Overview](#) and [Single-Session DHCP Dual-Stack Overview](#).]

- **Support for single-session DHCP dual-stack subscriber single BNG connect (MX Series)**—Starting in Junos OS Release 17.3R1, DHCP single-session dual-stack subscribers connect to a single broadband network gateway (BNG) in a load sharing access model.

For a DHCP dual-stack subscriber, the DHCPv4 and DHCPv6 protocol handshakes are generally completely independent of each other. So it is theoretically possible that each arm of a given dual-stack subscriber could connect to a different BNG. A configured mode of operation is supported to avoid this scenario

A given address family is designated as the protocol master for a dual-stack subscriber. Any binding attempt from the secondary address family client for a given dual-stack subscriber is rejected if a binding from the protocol master family of the same dual-stack subscriber is not currently active.

In case bindings for both arms of a DHCP dual-stack subscriber are currently active when the **protocol-master** family binding is released (or otherwise deleted for any reason), then the secondary address family binding for that subscriber will be automatically torn down.

[See [Single-Session DHCP Local Server Dual-Stack Overview](#) and [Single-Session DHCP Dual-Stack Overview](#).]

- **Support for DHCP local server dual-stack single-session (MX Series)**—Starting in Junos OS Release 17.3R1, DHCP local server dual-stack subscribers are supported on a single VLAN session. This reduces the required number of session database (SDB) entries utilized and simplifies RADIUS authentication and accounting operations.

The benefits of a single-session dual-stack model are as follows

- Simplifies router configuration.
- Reduces RADIUS message load.
- Reduces the backend correlation of multiple accounting sessions for the same household.
- Is Compatible with existing RADIUS messaging.

[See [Single-Session DHCP Local Server Dual-Stack Overview](#).]

- **Support for DHCPv6 prefix exclude option(MX Series)**—Starting in Junos OS Release 17.3R1, you can exclude one specific prefix that is bigger than the prefix length from a delegated prefix set while using DHCPv6 based prefix delegation. This specific prefix is used as the link between the delegating router and the requesting router, where the delegating router exchanges DHCPv6 messages with the requesting router. Configure the **exclude-prefix-len** statement at the **[edit access address-assignment pool delegated-address-pool family inet6 dhcp-attributes]** hierarchy level to exclude the prefix from the delegated prefix set. You can configure the **support-option-pd-exclude** statement at either the **[edit system services dhcp-local-server dhcpv6 reconfigure]** or the **[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]** hierarchy level to exclude prefix support in the reconfigure message.

[See [Understanding Support for DHCPv6 Prefix Exclude Option](#)]

EVPNs

- **EVPN-VXLAN support for VXLAN gateways using an IPv6 underlay (MX Series with MPC and MIC)**—Starting in Junos OS Release 17.3R1, MX Series routers with MPC and MIC interfaces extend support for Virtual Extensible LAN (VXLAN) gateways from IPv4 to IPv6 underlays. With this feature enhancement, each VXLAN gateway supports the following functionalities in addition to the IPv4 functionalities already supported:
 - VLAN-based service
 - VLAN-bundle service
 - Port-based service
 - VLAN-aware service

Similar to IPv4 underlay support, the IPv6 EVPN-VXLAN underlay supports the Type 2 MAC address with IP address advertisement and the proxy MAC address with IP address advertisement.

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

- **Preference-based DF election for EVPN and PBB-EVPN (MX Series with MPC and MIC interfaces)**—Starting in Junos OS Release 17.3, the designated forwarder (DF) election in a multihomed Ethernet VPN (EVPN) environment can be controlled using an administrative preference value for an Ethernet segment identifier (ESI). Currently, the DF election (as specified in RFC 7432) is performed randomly by all the multihoming devices using the modulo operation. With the preference-based DF election, the DF is elected manually using interface configuration options, such as the preference value and the router ID or loopback address. This method of DF election is useful when there is a need to choose the DF based on interface attributes like bandwidth associated with the interface.

To enable preference-based DF election, include the **df-election-type preference value value** statements at the **[edit interfaces interface-name esi]** hierarchy level.

[See [EVPN Multihoming Overview](#).]

- **Support for seamless migration from LDP-VPLS to EVPN (MX Series)**—Currently, a virtual private LAN service (VPLS) network can be connected to an Ethernet VPN (EVPN) network using logical tunnel interfaces on the interconnection point of the VPLS and EVPN routing instances. In this case, the provider edge (PE) devices in each network are unaware of the PE devices in the other technology network. Starting in Junos OS Release 17.3R1, a solution is introduced for enabling staged migration from FEC128 LDP-VPLS toward EVPN on a site-by-site basis for every VPN routing instance. In this solution, the PE devices running EVPN and VPLS for the same VPN routing instance and single-homed segments can coexist. During the migration, there is minimal impact to the customer edge (CE) device-to-CE device traffic forwarding for affected customers.

[See [Migrating From FEC128 LDP-VPLS to EVPN Overview](#).]

General Routing

- **Commit process split into two steps (MX Series)**—Starting in Junos OS Release 17.3R1, new configuration statements are introduced for **commit** to split the commit process into two steps. These configuration statements are **prepare** and **activate**.

In the first step, known as the preparation stage, **commit prepare** validates the configurations and then creates the necessary files and database entries so that the validated configurations can be activated at a later stage.

In the second step, referred to as the activation stage, **commit activate** activates the previously prepared commit. A new configuration statement, **prepared**, is added to **clear system commit**, which clears the prepared commit cache

This feature enables you to configure a number of Junos OS devices and simultaneously activate the configurations. This approach is helpful in time-critical scenarios.

[See [Commit Preparation and Activation Overview](#).]

High Availability (HA) and Resiliency

- **Mandatory action before initiating GRES in the presence of PIC bounce alarms (MX10003 router)**—In Junos OS Release 17.3R1, before initiating graceful Routing Engine switchover (GRES) on an MX10003, you must bounce the PIC (by issuing offline/online of the PIC) using [request chassis pic](#) command before performing switchover operation. Otherwise, it will provide negative results as the alarms are not preserved on GRES currently. It may also result in unstable behavior of MPC.

Consider the example of PIC bounce alarm shown below. In this case, you must bounce the PIC before initiating a switchover.

```
user@host# run show chassis alarms
Apr 17 01:50:13
4 alarms currently active
Alarm time           Class  Description
2017-04-17 01:48:57 PDT  Minor  FPC 0 PIC 1 Need bounce
2017-04-14 09:14:03 PDT  Major  PEM 4 Not Present
2017-04-14 09:14:03 PDT  Major  PEM 3 Not Present
2017-04-14 09:14:03 PDT  Major  PEM 1 Not Present
```

- **VRRP scale improvements per aggregated Ethernet bundle(MX Series)**—Starting in Junos OS Release 17.3R1, you can configure up to 4000 active VRRP sessions per aggregated Ethernet bundle on MX Series routers. To configure VRRP support, include the **vrrp-group** statement at the **[edit interfaces interface-name unit logical-unit-number family inet address ip-address]** hierarchy level.

[See [Understanding VRRP](#).]

Interfaces and Chassis

- **Support for new MX150 Universal Routing Platform**—Starting in Junos OS Release 17.3R1, Junos OS supports a new MX Series edge router—the MX150—which is a compact, high-performance edge router that is ideally suited for lower bandwidth service provider applications and distributed service architectures, and for enterprise WAN use-cases. The MX150 is 1 rack unit (RU) tall and supports bandwidth that can be upgraded from 100 Mbps to 20 Gbps.

- **Support for FRU control, power management, and environmental monitoring in MX10003 routers**—Starting with Junos OS Release 17.3R1, Junos OS chassis management software for the MX10003 routers provides enhanced environmental monitoring and FRU control. MX10003 has a pair of Routing Engines, which support virtualization. Each Routing Engine board is a single FRU. The MX10003 router has two MPCs, each supporting a bandwidth up to 1.2 Tbps. Each MPC has three Packet Forwarding Engines, each providing a maximum bandwidth of 400 Gbps. Each MPC supports a fixed PIC comprising six QSFP ports and a modular interface card (MIC) comprising 12 QSFP28 ports. All FRUs are upgradable. The MX10003 chassis has two power supply modules (PSM)—a DC PSM and an AC PSM. The MX10003 cooling system contains four fan assemblies, with two fans in each. MX10003 supports temperature thresholds for each temperature sensor, which enables the router to precisely control the cooling, raise alarms, and shut down an FRU. The router also supports preserving power-on sequence for the FPCs, and power management using ambient-temperature.

[See [Understanding How Dynamic Power Management Enables Better Utilization of Power.](#)]

- **Fabric management in MX10003 routers**—Starting with Junos OS Release 17.3R1, Junos OS supports management and control of fabric operations on MX10003 routers. On the MX10003 router, the switching fabric is located on the MPC. The router has two MPCs, each supporting a bandwidth up to 1.2 Tbps. The switching fabric has 22 planes and each plane supports a maximum link speed of 24.883 Gbps. MX10003 routers do not have a dedicated fabric card. The router supports features such as fabric hardening and forward error correction.

[See [MX Series Routers Fabric Resiliency.](#)]

- **MPCs, PICs, and MICs supported on MX10003 routers**—Starting with Junos OS Release 17.3R1, the MX10003 router supports a new MPC, MX10003 MPC. The MX10003 MPC supports three Packet Forwarding Engines. The forwarding capacity of each Packet Forwarding Engine is 400Gbps which cannot be oversubscribed. Each MPC supports a fixed-port PIC and modular MICs, JNP-MIC1 (MIC without MACsec support) and JNP-MIC1-MACSEC (MIC with MACsec support). The fixed port PIC is mapped to PIC 0 and each PFE is mapped to 2 ports in PIC 0. The MIC is mapped to PIC 1 and each PFE is mapped to 4 ports in PIC 1. The PIC/MIC ports on MX10003 router MPCs support multiple port speeds (10/40/100GE). Hence, these ports are classified as multi-rate ports. However, all the PIC/MIC ports do not support all the port speeds. On MPC all the 12 ports are active and are capable of running in 40-Gigabit Ethernet, 100-Gigabit Ethernet, and 4x10-Gigabit Ethernet mode. [See [MX10003 MPC on MX10003 Router Overview](#) for more details.]
- **Support for inline flow monitoring on MPCs on MX10003 routers**—Starting with Junos OS Release 17.3R1, MPCs on MX10003 router support inline flow monitoring. Inline flow monitoring results in higher scalability and performance, as the scaling and performance are not dependent on the capacity

of the services interface. MX10003 router contains two MPCs, each supporting a bandwidth up to 1.2 Tbps.

- **Broadband edge (BBE) telemetry sensors(MX Series)**—Starting in Junos OS Release 17.3R1, support is added for BBE telemetry sensors. These sensors are used to proactively manage a broadband network gateway (BNG) and are configured using both Junos Telemetry Interface (JTI) and gRPC streaming.

The new sensors are grouped into the following functional areas:

- Chassis and system extensions
 - AAA
 - DHCP
 - PPP
 - L2TP
 - MX Series routers Virtual Chassis
 - ERA
 - BBE infrastructure
 - Packet Forwarding Engine resource and monitoring
- **Support for inline NAT services on MX10003**—Starting with Junos OS Release 17.3R1, MX10003 routers support inline Network Address Translation (NAT) services on Modular Port Concentrators (MPCs). This enables you to achieve line-rate, low-latency address translations (up to 120 Gbps per slot) without having to use a dedicated MS-MPC for NAT.
 - **MAC address persistence after a Routing Engine switchover**—In Junos OS Release 17.3R1 and later, if you configure multiple aggregated Ethernet interfaces, the MAC addresses of the aggregated Ethernet interfaces are saved on a file that is stored on the master Routing Engine and is synchronized with the backup Routing Engine. The file is updated after each successful commit that required changes to the MAC addresses table.

In earlier releases, if you configure multiple aggregated Ethernet interfaces, the MAC address of the aggregated Ethernet interfaces displayed in the **show interfaces ae *number*** command output might get reordered after a Routing Engine switchover or restart.

- **Management Ethernet interface (fxp0) is confined in a non-default virtual routing and forwarding table (PTX 10008)**—Starting in Junos OS Release 17.3R1, you can confine the management interface in a dedicated management instance by setting a new CLI configuration statement, **management-instance**, at the **[edit system]** hierarchy level. By doing so, operators will ensure that management traffic no longer has to share a routing table (that is, the default.inet.0 table) with other control or protocol traffic in the system. Instead, there is a `mgmt_junos` routing instance introduced for management traffic.

[See [Management Interface in a Non-Default Instance](#) and [management-instance](#).]

IPsec

- **Support for configuring IPsec (site-to-site) VPN tunnels (MX150)**—Starting in Junos OS Release 17.3R1, the MX150 supports IPsec VPN connections or tunnels. You can configure a route-based VPN or a policy-based VPN. You implement a policy-based VPN if the remote VPN device is a non-Juniper Networks device and only one subnet or network at the remote site across the VPN needs to be accessed.

IPv6

- **IPv6 support (MX150)**—Starting in Junos OS Release 17.3R1, Junos OS supports IPv6 features on the MX150. The following is a list of some of the IPv6 features supported:
 - IPv6 forwarding
 - IPv6 path maximum transmission unit (MTU) discovery
 - Neighbor discovery
 - Static routes for IPv6
 - Internet Control Message Protocol (ICMP) version 6

Layer 2 Features

- **Support for Junos Fusion Provider Edge (MX10003 routers)**—Starting in Junos OS Release 17.3R1, you can configure MX10003 Universal Routing Platforms as aggregation devices in a Junos Fusion Provider Edge topology. Junos Fusion Provider Edge brings the Junos Fusion technology to the service provider edge. In a Junos Fusion Provider Edge, MX Series routers act as aggregation devices, while EX4300 and QFX5100 switches act as satellite devices.

[See [Understanding Junos Fusion Provider Edge Components.](#)]

- **Support for Layer 2 protocols on MX10003 routers**—Starting in Junos OS Release 17.3R1, all Layer 2 bridging features are supported on MX10003 routers.
- **Support for Layer 2 and Layer 3 features (MX150)**—Starting in Junos OS Release 17.3R1, the MX150 supports the following Layer 2 and Layer 3 features:
 - Layer 2 protocols and including Layer 2 Ethernet OAM and virtual private LAN service (VPLS)
 - VLAN support—VLANs enable you to divide one physical broadcast domain into multiple virtual domains.
 - Link Layer Discovery Protocol (LLDP)—Enables advertising the identity and capabilities on a LAN, and receive information about other network devices.
 - Layer 3 routing protocols and MPLS

Layer 2 VPN

- **Support of ping utility for testing CE device connectivity (MX Series with MPC and MIC)**—Starting in Junos OS Release 17.3R1, reachability to the customer endpoint can be achieved from the service endpoint in a network. This feature is supported in a virtual private LAN service (VPLS), hierarchical VPLS (H-VPLS), and Ethernet VPN (EVPN) network. It is based on the LSP ping infrastructure, where the **ping** utility is extended to use the CE device IP address as the target host and the PE device loopback address as the source for a specific VPLS or EVPN routing instance.

To implement this feature, issue the **ping ce-ip destination-ip-address instance routing-instance-name source-ip source-ip-address** command on a PE device. Based on the configured routing instance type, the command output displays the connectivity information of the CE device.

[See [Pinging Customer Edge Device IP Address.](#)]

- **Support for Group VPN (MX150)**—Starting in Junos OS Release 17.3R1, Junos OS supports Group VPN on the MX150. Group VPN extends existing IPsec architecture to support group-shared security associations. The group server manages group keys and policies and distributes them to group members. Group VPN provides the following benefits:
 - Data security and transport authentication.
 - High-scale network meshes, eliminating complex peer-to-peer key management with group encryption keys.
 - Full-time, direct communications between sites, without requiring transport through a central hub.

[See [Group VPN Overview.](#)]

- **Support for connectivity fault management**—Starting in Junos OS Release 17.3R1, Junos OS supports multiple up maintenance association end points (MEPs) for a single combination of maintenance association ID and maintenance domain ID for Layer 2 VPN local switching.

To configure multiple up MEPs, specify **mep mep-id** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance association ma-name]** hierarchy level, when the MEP direction is configured as **direction up**.

[See [Connectivity Fault Management Support for Layer 2 VPN.](#)]

- **Support for chained composite next hops**—Starting in Junos OS Release 17.3R1, you can enable composite chained next hops on MPCs on MX Series routers to manage ingress traffic for Layer 2 circuits and Layer 2 VPNs. A chained composite next hop allows the router to direct sets of routes sharing the same destination to a common forwarding next hop, rather than having each route also include the destination. This helps facilitate large volumes of traffic.

To enable composite chained next hop for ingress traffic, include the **l2ckt** or **l2vpn** statement at the **[edit routing-options forwarding-table chained-composite-next-hop ingress]** hierarchy level.

[See [Chained Composite Next Hops for Layer 2 VPNs and Layer 2 Circuits.](#)]

Layer 3 Features

- **Junos Fusion support (MX2008)**—Starting in Junos OS Release 17.3R1, the Junos OS supports a network system named Junos Fusion. Based on the 802.1BR standard, Junos Fusion is a combination of aggregation devices and satellite devices that appear to the rest of the network as a single device. Junos Fusion expands the port density of the aggregation device and allows it to send and receive traffic using the customer-facing ports of the directly connected satellite devices. The composite of the aggregation device and satellite devices—the Junos Fusion—is configured and managed through the aggregation device. You can configure MX2008 Universal Routing Platforms as an aggregation device.

[See [Junos Fusion Provider Edge Overview](#).]

- **Support for Layer 3 protocols(MX10003)**—Starting in Junos OS Release 17.3R1, Layer 3 protocols are supported on MX10003 routers. Layer 3 protocols include the Multiprotocol Label Switching (MPLS), Layer 3 Virtual Private Network (L3VPN), Bidirectional Forwarding Detection (BFD), Layer 2 Virtual Private Network (L2VPN), Point-to-multipoint (P2MP), fast reroute (FRR), Operations, Administration and Maintenance (OAM), Protocol Independent Multicast (PIM), Internet Group Management Protocol (IGMP), Adaptive Load Balancing (ALB), and so on.

Management

- **Support for Junos Telemetry Interface (MX150)**—Starting with Junos OS Release 17.3R1, the Junos Telemetry Interface is supported on the MX150 router. Junos Telemetry Interface enables you to provision sensors to stream telemetry data for network elements without involving polling.

On the MX150 router, only the following sensors are supported:

- Physical interfaces (UDP and gRPC streaming)
- Network Discovery Protocol table state (gRPC streaming only)
- Address Resolution Protocol table state (gRPC streaming only)
- IPFIX inline flow aggregation (UDP streaming only)
- Chassis components (gRPC streaming only)

To provision sensors to stream data through UDP, all parameters are configured at the **[edit services analytics]** hierarchy level. To provision sensors to stream data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters for a specified list of OpenConfig commands paths. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models.

[See [Overview of the Junos Telemetry Interface](#).]

- **Support to configure YANG files for Junos Telemetry Interface (MX Series)**—Starting with Junos OS Release 17.3R1, you can add user-defined YANG files that provide mappings between the XML path and the OpenConfig path for data streamed through the Junos Telemetry Interface. Previously, only the Junos OpenConfig package was available for providing these mappings to the XML proxy for data streamed through gRPC. To add YANG files, include the **request system yang add package package-name proxy-xml module yang-file-path** operational command. You can validate the YANG module by using

the **request system yang validate proxy-xml module *yang-file-path*** command. To delete a YANG file, use the **request system yang delete package *package-name* proxy-xml *yang-file-path*** operational command.

[See [Creating YANG Files for XML Proxy for Junos Telemetry Interface.](#)]

- **Enhancements to BGP peer sensors for Junos Telemetry Interface (MX Series)**—Starting with Junos OS Release 17.3R1, telemetry data streamed through gRPC for BGP peers is reported separately for each routing instance. To export data for BGP peers, you must now include the following path in front of all supported paths: **/network-instances/network-instance/[name_'*instance-name*']/protocols/protocol/**

Additionally, the following paths are also now supported:

- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi/state/prefixes/accepted**
- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/snmp-peer-index**
- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi/state/queues/output**
- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi/state/queues/input**
- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/state/ImportEval**
- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/state/ImportEvalPending**

Use the **telemetrySubscribe** RPC to specify telemetry parameters and provision the sensor. If your device is running a version of Junos OS with an upgraded FreeBSD kernel, you must download the Junos Network Agent software package, which provides the interfaces to manage gRPC subscriptions.

[See [Guidelines for gRPC Sensors.](#)]

- **Support for packet loss priority for Junos Telemetry Interface (MX Series)**—Starting with Junos OS Release 17.3R1, you can specify loss priority for telemetry packets streamed through UDP only. Loss priority settings help determine which packets are dropped from the network during periods of congestion. To configure, include the **loss-priority (high | low | medium-high | medium-low)** statement at the **[edit services analytics export-profile *profile-name*]** hierarchy level. To apply an export profile to a sensor, include the **export-name *profile-name*** statement at the **[edit services analytics sensor *sensor-name*]** hierarchy level. The **show agent sensors** command includes a new **loss-priority** field that is displayed for each sensor when this new option is configured.

[See [Configuring a Junos Telemetry Interface Sensor.](#)]

- **Junos Telemetry Interface support (MX10003 and MX204)**—Starting with Junos OS Release 17.3R1, MX10003 and MX204 routers support the Junos Telemetry Interface, which enables you to provision sensors to export telemetry data for various network elements. To provision sensors to stream data through UDP, all parameters are configured at the **[edit services analytics]** hierarchy level. To provision

sensors to stream data through gRPC, use the telemetrySubscribe RPC to specify telemetry parameters for a specified list of OpenConfig command paths. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models.

MPLS

- **Anchor point redundancy support for pseudowire subscriber logical Interfaces (MX Series)**—Starting in Junos OS Release 17.3R1, stateful anchor point redundancy support is provided for pseudowire subscriber logical interfaces by the underlying redundant logical tunnel interface in active-backup mode. This redundancy protects the access and the core facing link against anchor Packet Forwarding Engine failure.

Both transport and services logical interfaces created for the pseudowire subscriber logical interface are stacked on the underlying redundant logical tunnel control logical interface. This logical interface stacking model is used for both redundant and non-redundant pseudowire subscriber logical interfaces.

[See [Anchor Redundancy Pseudowire Subscriber Logical Interfaces Overview](#).]

- **Support for features on MPC7E, MPC8E, and MPC9E line cards (MX Series)**—In Junos OS Release 17.3R1, MPC7E, MPC8E, and MPC9E support the following features:

- LDP uses the longest match to learn the routes aggregated or summarized across OSPF areas or IS-IS levels in the interdomain.
- Support for notifications on the service node when the access pseudowire goes down, and efficient termination capabilities when Layer 2 and Layer 3 segments are interconnected.

[See [Pseudowire Termination: Explicit Notifications for Pseudowire Down](#).]

- BGP PIC Edge for RSVP enables you to implement a solution where a protection path is calculated in advance to provide an alternative forwarding path in case of path failure.

[See [show rsvp version](#).]

- Circuit cross-connect (CCC) encapsulation is supported on the transport side of an MPLS pseudowire subscriber logical interface. This feature helps in migrating or deploying seamless MPLS architectures in access networks.

[See [Pseudowire Subscriber Logical Interfaces Overview](#).]

- inet and inet6 families are supported on the services side of an MPLS pseudowire subscriber as well as non subscriber logical interfaces.
- Distributed denial-of-service (DDoS) protection is supported on the services side of an MPLS pseudowire subscriber logical interface.
- Policer and filter are supported on the services side of an MPLS pseudowire subscriber logical interface.
- Accurate transmit logical interface statistics are supported on the services side of an MPLS pseudowire subscriber logical interface.

- Inline IPFIX is supported on the services side of an MPLS pseudowire subscriber logical interface.
- Port mirroring is supported on the services side of an MPLS pseudowire subscriber logical interface.

Multicast

- **PIM resolve type-length-value (TLV) for multicast in seamless MPLS (MX Series)**—Starting in Junos OS Release 17.3R1, Junos OS adds support for RFC 5496, Reverse Path Forwarding (RPF) Vector TLV . With this support, Protocol Independent Multicast (PIM) can be used in environments where the core routers do not maintain external routes, for example in a seamlessMPLS network.

[See [rpf-vector](#).]

- **Support for IPv6 multicast Rosen version 7 (MX Series)**—Starting in Junos OS Release 17.3R1, Junos OS multicast support extends to the default multicast distribution tree (MDT) for Rosen 7 multicast virtual private networks (MVPN) and data MDT for both Rosen 6 (PIM-ASM) and Rosen 7 (PIM-SSM). The IPv6 support applies to the customer space only.

[See [Draft-Rosen Multicast VPNs Overview](#) .]

Network Management and Monitoring

- **mLDP MIB extends support to LDP point-to-multipoint (P2MP) LSPs (MX Series)**—Starting in Junos OS Release 17.3R1, the mLDP MIB builds on the objects and tables that are defined in RFC 3815, which only support LDP point-to-point label switched paths (LSPs). This mLDP MIB provides support for managing multicast LDP point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) LSPs. The mLDP MIB tables are directly accessible through SNMP. All objects in the mLDP MIB are read-only and cannot be created or set through SNMP. This implementation of mLDP MIB is specified in draft-ietf-mpls-mlbp-mib.
- **Support for automatic targeted distribution of logical interface sets of static VLANs over aggregated ethernet logical interfaces (MX Series)**—Starting in Junos OS Release 17.3R1, automatic targeted distribution of logical interface sets of static VLANs over aggregated Ethernet logical interfaces is supported. When targeted distribution is set for a logical interface sets then the logical interface set participates in targeting and the link selected for the logical interface set is propagated to the underlying logical interfaces. You can assign weight for all the targeted subscribers like PPPoE, demux, and conventional VLANs based on the business, CoS, or bandwidth requirement. To configure the **weight** statement at either the **[edit interfaces interface-set interface-set-name targeted-options]** or the **[edit interfaces interface-name unit unit-number targeted-options]** hierarchy level to assign the member links for the logical interface set or logical interface based on the weight value.

[See [Understanding Support for Targeted Distribution of Logical Interface Sets of Static VLANs over Aggregated Ethernet Logical Interfaces](#).]

- **Support for inline jflow version 9 flow templates (PTX1000)**—Starting in Junos OS Release 17.3R1, you can use inline-JFlow's export capabilities with version 9 flow templates to define a flow record template suitable for IPv4 or IPv6 traffic.

[See [Configuring Flow Aggregation to Use Version 9 Flow Templates on PTX Series Routers](#).]

Operation, Administration, and Maintenance (OAM)

- **Junos OS daemons to natively emit JSON output (MX Series)**—Starting with Junos OS Release 17.3R1, the operational state emitted by daemons is supported in JSON format as well as XML format. To configure JSON format, specify the following CLI command: **set system export-format state-data json compact**. To specify JSON format for specific command output, include **display json** in specific CLI commands.
- **Support for Ethernet OAM Rx statistics for CCM (MX Series)**—Starting in Junos OS Release 17.3R1, the **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md-name maintenance-association ma-id local-mep mep-id remote-mep mep-id** command displays Ethernet OAM Rx statistics. The Ethernet OAM Rx statistics displays the number of CCM PDUs received for a particular maintenance association and remote MEP and does not include error packets received.

NOTE: The Ethernet OAM Rx statistics are not displayed for UP MEP on trunk modes if the network-services mode is configured as IP.

If you perform unified ISSU, the counter is reset to zero. The counter is also reset to zero when the session flaps or if the session is down.

NOTE: If you do not provide the local MEP and remote MEP IDs, the **show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md-name maintenance-association ma-id local-mep mep-id remote-mep mep-id** command does not display latest statistics. Also, if you do not provide the remote MEP ID, then actual received statistics display zero.

- **Support for connectivity fault management (CFM) monitoring between customer-edge (CE) and provider-edge (PE) devices (MX Series)**—Starting in Junos OS Release 17.3R1, you can enable CFM monitoring between PE devices and CE devices when the CE device is not a Juniper Networks device by using the remote defect indication (RDI) bit. When the status of the EVPN provider edge device is standby, the EVPN VPWS service is notified and it sets the interface status to CCC-down. When the interface status is CCC-down, it indicates that the PE service is down. When you enable CFM monitoring, CFM propagates the status of the PE device via the RDI bit in the CC messages. Thus, the CE device is aware that the PE device is down. The RDI bit is cleared when the service is back up.

To enable CFM monitoring by using the RDI bit, use the **interface-status-send-rdi** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name maintenance-association ma-name continuity-check]** hierarchy level.

Alternately, you can enable CFM monitoring by using the **interface-status-tlv** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name maintenance-association ma-name continuity-check]** hierarchy level.

- **Nonstop active routing support for link fault management (LFM) (MX Series)**—Starting in Junos OS Release 17.3R1, the Ethernet link fault management daemon (lfmd) runs on the backup Routing Engine as well when GRES is configured. When the lfmd daemon runs on the backup Routing Engine as well, the LFM states are kept in sync and so minimal work is required by the lfmd daemon after switching over. To verify if the LFM states are in sync, use the **show oam ethernet link-fault-management** command on both master and backup Routing Engines. In Junos OS Release 17.2R1 and earlier, the lfmd daemon runs only on the master Routing Engine when GRES is configured.
- **Junos OpenConfig to support adjacent RIB operational state model (MX Series)**—Starting with Junos OS Release 17.3R1, **adj-rib-in-pre** and **adj-rib-out-post** tables have been added for the OpenConfig RIB operational state mode. The BGP RIB consists of several tables per address family, consisting of **loc-rib** and **per-neighbor** tables.
- **Support for inline CCM and BFD on MX10003 routers**—MX10003 routers support inline transmission of continuity check messages (CCMs) to achieve maximum scaling of CCMs. By enabling inline transmission of CCMs, you can delegate transmission of CCMs to the forwarding ASIC (that is, to the hardware). Inline transmission enables the system to handle more connectivity fault management (CFM) sessions per line card. MX10003 routers also support the Bidirectional Forwarding Detection (BFD) protocol, which is a mechanism that detects failures in a network.

Port Security

- **Media Access Control Security (MACsec) support on Terabit Interface card (MX10003)**—Starting in Junos OS Release 17.3R1, Junos OS supports MACsec on the 12x QSFP28 Terabit Interface card (TIC) in MX10003 routers. MACsec is an industry-standard security technology that provides secure communication for all traffic on point-to-point Ethernet links. MACsec is capable of identifying and preventing most security threats, and can be used in combination with other security protocols to provide end-to-end network security. MACsec can be enabled only on domestic versions of Junos OS software. MACsec is standardized in IEEE 802.1AE.

Routing Policy and Firewall Filters

- **Support for packet forwarding features (MX150)**—Starting in Junos OS Release 17.3R1, the MX150 supports the following key packet forwarding features:
 - **Basic Layer 2 features and protocols**—You can configure layer 2 features that can vary from the very simple (aggregated Ethernet trunk interfaces, spanning trees), to the more complex (inner and outer VLAN tags, broadcast domains), to the very complicated (integrated bridging and routing, layer 2 filtering).
 - **Class of service (CoS)**—You can configure CoS features to provide multiple classes of service for different applications. CoS enables you to divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs. It enables you to provide differentiated services when best-effort traffic delivery is insufficient.
 - **Firewall filters and policers**—You can configure firewall filters that define whether to accept or discard packets. You can use firewall filters on interfaces, VLANs, routed VLAN interfaces (RVIs), link aggregation

groups (LAGs), and loopback interfaces. You can use policing to apply limits to traffic flow and specify the action to be taken for packets that exceed those limits.

- **Port mirroring**—Port mirroring copies packets entering or exiting a port or entering a VLAN and sends the copies to a local interface for local monitoring. You can use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on.
- **Bypass loopback with firewall filter tunnel encapsulation (MX Series)**—Starting in Junos OS Release 17.3R1, static filter based generic routing encapsulation (GRE) tunnels no longer use a loopback stream for transit traffic. The new default, which allows for increased bandwidth utilization on MPCs using the MX Series chipset, is to skip the loopback. In addition, support for IPv4 as the outer IP is available (the inner payload supports both IPv4 and IPv6). Egress sampling on the outer header is not affected. This change does not apply to GRE in UDP or to dynamic tunnels.

This change applies to the following filter-based tunneling commands in the CLI:

```
set firewall family inet6 filter filter term term then encapsulate tunnel
```

```
set firewall tunnel-end-point tunnel ipv4 source-address ipv4 address
```

```
set firewall tunnel-end-point tunnel ipv4 destination-address ipv4 address
```

```
set firewall tunnel-end-point tunnel gre
```

[See [Filter-Based Tunneling Across IPv4 Networks](#).]

- **Hop-limit firewall filter match condition supported (PTX1000)**—Starting in Junos OS Release 17.3R1, you can configure a firewall filter using the hop-limit and hop-limit except match conditions for IP version 6 (IPv6) traffic (family inet6).

NOTE: The hop-limit and hop-limit except match conditions are supported on PTX1000 routers when [enhanced-mode](#) is configured on the router.

[See [Firewall Filter Match Conditions for IPv6 Traffic](#).]

- **Support for Hop-limit firewall filter match condition (PTX10008)**—Starting in Junos OS Release 17.3R1, you can configure a firewall filter using the **hop-limit *hop-limit*** and **hop-limit except *hop-limit*** match conditions for Internet Protocol version 6 (IPv6) traffic (family inet6).

NOTE: The **hop-limit *hop-limit*** and **hop-limit except *hop-limit*** match conditions are supported on PTX series routers when you configure the network-services mode as **enhanced-mode** on the router.

For more information, see [Firewall Filter Match Conditions for IPv6 Traffic](#).

Routing Protocols

- **Support for timing and synchronization on Terabit Interface card (MX10003)**—Starting in Junos OS Release 17.3R1, 12x QSFP28 Terabit Interface card (TIC) in MX10003 routers support the following timing and synchronization features:
 - **SyncE support with ESMC**—Synchronized Ethernet with Ethernet synchronization Message Channel (ESMC) is supported as per the ITU G.8264 specification. ESMC is a logical communication channel. It transmits synchronization status message information, which is the quality level of the transmitting synchronous Ethernet equipment clock, by using ESMC protocol data units.
 - **PTP support**—Precision Time Protocol (PTP), also known as IEEE 1588v2, is a packet-based technology that enables the operator to deliver synchronization services on packet-based mobile backhaul networks. IEEE 1588 PTP (Version 2) clock synchronization standard is a highly precise protocol for time synchronization that synchronizes clocks in a distributed system. The time synchronization is achieved through packets that are transmitted and received in a session between a master clock and a slave clock. One step clock mode operation for the master clock is supported.
 - **BITS (T1/E1) Interface support**—BITS support for input and output on T1/E1 framed and 2.048MHz unframed clock input.
 - **GPS external clock interface and TOD support**—GPS input and output support for 1 MHz/5 MHz/10 MHz and PPS signal .

[See [Ethernet Synchronization Message Channel Overview](#)].

- **Routing protocol process (rpd) recursive resolution over multipath (MX Series)**—Starting in Junos OS Release 17.3R1, when a BGP prefix that has a single protocol next hop is resolved over another BGP prefix that has multiple resolved paths (unilist), all the paths are selected for protocol next-hop resolution. In prior Junos OS releases, only one of the paths is picked for protocol next-hop resolution. This new feature benefits densely connected networks where BGP is used to establish infrastructure connectivity such as WAN networks with high equal-cost multipath and seamless MPLS topology.

To configure recursive resolution over multipath, define a policy that includes the **multipath-resolve** action at the **[edit policy-options policy-statement *policy-name* then]** hierarchy level and import the policy at the **[edit routing-options resolution rib *rib-name*]** hierarchy level.

Currently, if you apply the policy on **bgp.l2vpn.0** only, the RIB, also known as the routing table reflects recursively resolved multiple paths only in the control plane, you need to explicitly apply the policy on **mpls.0** to reflect recursively resolved multiple paths on the data plane also.

[See [Configuring Recursive Resolution over BGP Multipath](#).]

- **Redistribution of IPv4 routes over IPv6 routes into BGP through tunnels (MX Series)**—Starting in Release 17.3R1, Junos OS devices can forward IPv4 traffic over an IPv6-only network, which generally cannot forward IPv4 traffic. As described in RFC 5549, IPv4 traffic is tunneled from CPE devices to IPv4-over-IPv6 gateways. These gateways are announced to CPE devices through anycast addresses. The gateway devices then create dynamic IPv4-over-IPv6 tunnels to remote CPE devices and advertise IPv4 aggregate routes to steer traffic. Route reflectors with programmable interfaces inject the tunnel information into

the network. The route reflectors are connected through IBGP to gateway routers, which advertise the IPv4 addresses of host routes with IPv6 addresses as the next hop. Currently the dynamic IPv4-over-IPv6 tunnel feature does not support unified ISSU.

To configure a dynamic IPv4-over-IPv6 tunnel, include the **dynamic-tunnels** statement at the **[edit routing-options]** hierarchy level.

[See [Understanding Redistribution of IPv4 Routes with IPv6 Next Hop into BGP.](#)]

- **Support for IS-IS SPRING and RSVP coexistence (MX Series)**—Starting in Junos OS Release 17.3R1, the routing protocol process (rpd) takes into account the bandwidth used by SPRING traffic to calculate the balance bandwidth available for RSVP-TE. The allocated bandwidth for RSVP is periodically modified based on the traffic on the SPRING interface and its bandwidth utilization. To configure automatic bandwidth calculation, include the **auto-bandwidth template** statement at the **[edit routing-options]** hierarchy level. You can apply the **auto-bandwidth template** configuration either globally at the **[edit protocols isis source-packet-routing traffic-statistics]** hierarchy level or at the **[edit protocols isis interface *interface-name*]** hierarchy level. This feature is useful for networks that are moving to SPRING but also have RSVP deployed, and continue to use both SPRING and RSVP.

[See [auto-bandwidth.](#)]

- **Support for BGP large communities (MX Series)**—Starting in Junos OS Release 17.3R1, BGP community is enhanced to support a BGP large community, which uses 12-byte encoding. The most significant 4 bytes encode an autonomous system number or global administrator and the remaining two 4 bytes encode operator defined local values. Currently, BGP normal community (4 byte) and BGP extended community (6 byte) provide limited support for BGP community attributes after the introduction of a 4 byte autonomous system number. Configure the large BGP community attributes at the **[edit policy-options community *community-name* members]** hierarchy level and at the **[edit routing-options static route *route* community]** hierarchy level with keyword **large** followed by three 4-byte unsigned integers separated by colons. The attributes are represented as large:autonomous system number:local value 1:local value2.

[See [Understanding BGP Communities, Extended Communities, and Large Communities as Routing Policy Match Conditions](#)]

- **Support for inline Two-Way Active Measurement Protocol (TWAMP) server and client on MX10003 routers**—Starting in Junos OS Release 17.3R1, supports the inline Two-Way Active Measurement Protocol (TWAMP) control-client and server for transmission of TWAMP IPv4 UDP probes between the session-sender (control-client) and the session-reflector(server). The TWAMP control-client and server can also work with a third-party server and control-client implementation. TWAMP is an open protocol for measuring network performance between any two devices that support TWAMP.

Security

- **Secure boot (MX10003)**—Starting in Junos OS Release 17.3R1, a significant system security enhancement, secure boot, has been introduced. The secure boot implementation is based on the UEFI 2.4 standard. The BIOS has been hardened and serves as a core root of trust. The BIOS updates, the bootloader, and the kernel are cryptographically protected. secure boot is enabled by default on supported platforms.

Services Applications

- **ECDSA authentication for IKE SA and AES-GCM encryption for IPsec SA (MX Series routers with MS-MPCs and MS-MICs)**—Starting in Junos OS Release 17.3R1, you can configure the Elliptic Curve Digital Signature Algorithm (ECDSA) authentication method for an IKE security association (SA) and the Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) encryption algorithm for an IPsec SA for MS-MPCs and MS-MICs. Junos OS supports the ECDSA 256-bit and 384-bit moduli methods and the AES-GCM 128-bit, 192-bit, and 256-bit encryption algorithms.

[See [Configuring IKE Proposals](#) and [Configuring IPsec Proposals](#).]

- **Support for IPv6 GRE tunnels (MX Series)**—Starting in Junos OS Release 17.3R1, you can configure IPv6 generic routing encapsulation (GRE) tunnel interfaces on MX Series routers. This lets you run a GRE tunnel over an IPv6 network. Packet payload families that can be encapsulated within the IPv6 GRE tunnels include IPv4, IPv6, MPLS, and ISO. Fragmentation and reassembly of the IPv6 delivery packets is not supported.

To configure an IPv6 GRE tunnel interface, specify IPv6 addresses for **source** and **destination** at the **[interfaces gr-0/0/0 unit 0 tunnel]** hierarchy level.

[See [GRE Keepalive Time Overview](#).]

- **Increased number of IPv4 RPM probes (MX Series with MS-MPCs and MS-MICs)**—Starting in Junos OS Release 17.3R1, you can increase the number of IPv4 **icmp-ping** and **icmp-ping-timestamp** real-time performance monitoring (RPM) probes that can run simultaneously. Use the **delegate-probes** statement to configure an MS-MPC or MS-MIC services interface to perform the RPM processing for the probes, enabling more probes to run simultaneously.

[See [Configuring RPM Probes](#).]

- **Inline TWAMP requester support (MX2010 and MX2020 routers)**—Starting in Junos OS Release 17.3R1, MX2010 and MX2020 routers support the inline Two-Way Active Measurement Protocol (TWAMP) control-client and session-sender for transmission of TWAMP probes using IPv4 between the sender (control-client or session-sender) and the receiver (server or session-reflector). The control-client and session-sender reside on the same router. The TWAMP control-client can also work with a third-party server implementation.
- **Support for enhancing the current Inline JFlow scale limits for XL-based and EA-based linecards for MX routers**—Starting in Junos OS Release 17.3R1, the **ipv4-flow-table-size**, **ipv6-flow-table-size**, **vpls-flow-table-size**, and **mpls-flow-table-size** allow upto 245 **flow-table-size** to support 64M flows at the **[edit chassis fpc slot-number inline-services flow-table-size]** hierarchy level. The existing limit on

flow-export-rate under **inline-jflow** for each family in the sampling instance is increased to 3200 from 400.

- **Support for Inline services (MX150)**—Starting in Junos OS Release 17.3R1, the MX150 supports inline active flow monitoring services. Inline active flow monitoring provides for higher scalability and performance and is implemented on the Packet Forwarding Engine. Version 9 template and IP Flow Information Export (IPFIX) template are supported to define a flow record template suitable for IPv4 or IPv6 traffic.

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

- **RPM support for IPsec and GRE tunnels (MX Series router with MS-MPCs and MS-MICs)**—Starting in Junos OS Release 17.3R1, you can apply real-time performance monitoring (RPM) to IPsec tunnels and GRE tunnels for PIC-based and Routing Engine based RPM clients and servers if you are using MS-MPCs or MS-MICs. Packet Forwarding Engine based RPM is not supported for IPsec tunnels. Support of RPM on IPsec tunnels enables service-level agreement (SLA) monitoring for traffic transported in IPsec tunnels.

[See [Real-Time Performance Monitoring Services Overview](#).]

- **NAT with deterministic IP address and port mapping (MX Series routers with MS-MPCs and MS-MICs)**—Starting in Junos OS Release 17.3R1, support for deterministic NAT mapping for NAPT44 is extended to the MS-MPC and MS-MIC. Deterministic NAT mapping ensures that a given internal IP address and port are always mapped to the same external IP address and port range, and the reverse mapping of a given translated external IP address and port are always mapped to the same internal IP address. Deterministic NAT mapping eliminates the need for logging address translations.

[See [Configuring Deterministic NAPT](#).]

- **Support for TWAMP server and client (MX150)**—Starting in Junos OS Release 17.3R1, the MX150 supports the inline Two-Way Active Measurement Protocol (TWAMP) control-client and server for transmission of TWAMP IPv4 UDP probes between the session-sender (control-client) and the session-reflector (server). The TWAMP control-client and server can also work with a third-party server and control-client implementation. TWAMP is an open protocol for measuring network performance between any two devices that support TWAMP.

[See [Two-Way Active Measurement Protocol Overview](#).]

- **Increase in IKE tunnel setup rate (MX Series routers with MS-MPCs and MS-MICs)**—Starting in Junos OS Release 17.3R1, the IKE tunnel setup rate has increased if you are using MS-MPCs or MS-MICs. This increase is the result of moving the public key cryptographic operations to the MS-MPC or MS-MIC.

[See [Understanding Junos VPN Site Secure](#).]

- **Maximum number of RPM probes increased (MX Series routers)**—Starting in Junos OS Release 17.3R1 and 17.2R2, you can configure the maximum allowed number of concurrent real-time performance monitoring (RPM) probes on an MX Series router to be as high as 2000. In Junos OS Release 17.2R1 and earlier, you can configure the maximum number to be as high as 500.

[See [Limiting the Number of Concurrent RPM Probes](#).]

Software Defined Networking (SDN)

- **Support for Junos Node Slicing on MX480 routers**—Starting with Junos OS Release 17.3R1, MX480 routers support Junos Node Slicing. Junos node slicing is the capability to partition an MX Series router to make it appear as multiple, independent routers. Each partition has its own independent Junos OS control plane and dataplane, which run as a virtual machine (VM), and a dedicated set of line cards. Each partition is called a guest network function (GNF). In the node slicing setup, the MX Series router functions as the base system (BSYS). Junos node slicing enables the convergence of multiple services on a single physical infrastructure while avoiding the operational complexity involved.

[See [Junos Node Slicing](#).]

- **Support for OpenDaylight (ODL) controller on MX Series routers**—Starting with Junos OS Release 17.3R1, MX Series router supports OpenDaylight (ODL) controller (Boron-SR1 release), which provides an open source platform for network programmability aimed at enhancing software-defined networking (SDN). The ODL controller provides a southbound Network Configuration Protocol (NETCONF) connector API, which uses NETCONF and YANG models to interact with a network device. You can use the ODL controller to orchestrate and provision MX Series routers, and execute remote procedure calls (RPCs) to the routers to get state information. Also, the ODL controller enables you to carry out configuration changes in the routers. To configure the ODL controller to interoperate with MX Series routers, include the **netconf rfc-compliant** and **netconf yang-compliant** statements at the **[edit system services]** hierarchy level.

[See [Configuring Interoperability Between MX Series Routers and OpenDaylight](#)]

- **Advanced Forwarding Interface (AFI) API is available for vMX routers**—Starting in Junos OS Release 17.3R1, the Advanced Forwarding Interface (AFI) version 1.0 is available for vMX routers. AFI APIs are provided as C++ APIs only. The APIs allow developers to interact with the Packet Forwarding Engine by accessing a section of the forwarding path from within a sandbox to affect the traffic that enters that part of the path. The sandbox is provided by Junos OS after CLI-based configuration and has one or more pairs of input and output ports that represent the points along the forwarding path at which the AFI clients enter and exit the path to do their work.

Subscriber Management and Services

- **Support for excluding tunnel attributes from RADIUS Access-Request messages (MX Series)**—Starting in Junos OS Release 17.3R1, you can use the **exclude** statement at the **[edit access profile profile-name radius attribute]** hierarchy level to exclude the following tunnel attributes from RADIUS Access-Request messages in addition to the previously supported Accounting-Start and Accounting-Stop messages:
 - **acct-tunnel-connection**—RADIUS attribute 68, Acct-Tunnel-Connection
 - **tunnel-assignment-id**—RADIUS attribute 82, Tunnel-Assignment-Id
 - **tunnel-client-auth-id**—RADIUS attribute 90, Tunnel-Client-Auth-Id
 - **tunnel-client-endpoint**—RADIUS attribute 66, Tunnel-Client-Endpoint
 - **tunnel-medium-type**—RADIUS attribute 65, Tunnel-Medium-Type
 - **tunnel-server-auth-id**—RADIUS attribute 91, Tunnel-Server-Auth-Id

- tunnel-server-endpoint—RADIUS attribute 67, Tunnel-Server-Endpoint
- tunnel-type—RADIUS attribute 64, Tunnel-Type

[See [Configuring How RADIUS Attributes Are Used for Subscriber Access.](#)]

- **Clearing accounting option statistics from the Packet Forwarding Engine (MX Series)**—Starting in Junos OS Release 17.3R1, you can issue the **clear interfaces statistics *interface-name*** command to clear counters for accounting statistics received on the logical interface from the Packet Forwarding Engine. The existing statistics are stored as the new current baseline statistics and the counters are reset to zero. This applies to interfaces for which accounting statistics are collected as specified by the **interface-profile** statement at the **[edit accounting-options]** hierarchy level.

Include the **allow-clear** statement in the interface profile to enable reporting of the cleared (new current baseline) statistics to the accounting flat file. Reporting is disabled by default. When you clear statistics for an interface that does not have this statement in its interface profile, the CLI displays the statistics as cleared, but this is not reported to the flat file.

[See [Configuring the Interface Profile.](#)]

- **Filter actions extended to dynamic filters (MX Series)**—Starting in Junos OS Release 17.3R1, you can include the **dscp *value*** action for the inet address family and the **traffic-class *value*** action for the inet6 address family in dynamic, parameterized filters. This means that you can configure a user-defined dynamic variable or a static value for the action value. In earlier releases, these actions are supported only for static (nonparameterized) filters.

[See [Parameterized Filter Nonterminating and Terminating Actions and Modifiers.](#)]

- **Support for inline IP reassembly on GRE tunnel interfaces (MX Series routers with MPCs)**—Starting in Junos OS Release 17.3R1, you can configure fragmentation and inline reassembly of generic routing encapsulation (GRE) packets on GRE tunnel interfaces on MX Series routers with the following Modular Port Concentrators: MPC7E, MPC8E, and MPC9E.

[See [Enabling Fragmentation and Reassembly on Packets After GRE-Encapsulation](#)]

- **Limiting subscribers based on client type for different hardware elements (MX Series)**—Starting in Junos OS Release 17.3R1, use the **subscribers-limit** stanza at the **[edit system services resource-monitor]** hierarchy level to configure the maximum number of subscribers by client type (DHCP, L2TP, PPPoE, or the sum of all three) that are allowed per chassis, MPC, MIC, and port. Subscriber login is denied when the number of subscribers having that type exceeds the configured limit. This feature ensures that the number of subscribers per hardware element does not exceed the number that your network can serve with stability at the desired bandwidth. When the limit is reached for a hardware element, new subscribers can connect to another hardware element in the same broadcast domain. When you configure the limit on one or more legs of an aggregated Ethernet interface, login is denied if the subscriber count exceeds the value on any of the legs.

Use the **show system resource-monitor subscribers-limit** command to display information about subscriber limits.

[See [Limiting Subscribers by Client Type and Hardware Element with Resource Monitor.](#)]

- **Support for sending LAC NAS-port and LAC IP-address attributes to RADIUS for MX Routers**—Starting in Junos OS Release 17.3R1, you can override the following at the `[edit access profile set radius options override]` hierarchy level:

- **nas-port** with the LAC side **nas-port** information.
- **nas-ip-address** with the l2tp LAC endpoint IP address information.

- **Support for load-based throttling of subscribers (MX Series)**—Starting in Junos OS Release 17.3R1, the **no-load-throttling** statement disables line card load-based throttling when configured at the `[edit system services resource-monitor]` hierarchy level. Load-based throttling is also disabled when the **no-throttle** statement is configured at the `[edit system services resource-monitor]` hierarchy level.

- **DDoS protection flow detection for enhanced subscriber management (MX Series Routers)**—Starting in Junos OS Release 17.3R1, enhanced subscriber management supports flow detection for DDoS protection. Enable flow detection by including the **flow-detection** statement at the `[edit system ddos-protection global]` hierarchy level. Flows that violate a DDoS protection policer are tracked as suspicious flows; they become culprit flows when they violate the policer bandwidth for the duration of a configurable detection period. Culprit flows are dropped, kept, or policed to below the allowed bandwidth level. Suspicious flow tracking stops if the violation stops before the detection period expires.

Most flow detection attributes are configured at the packet level or flow aggregation level of the CLI hierarchy (`[edit system ddos-protection protocols protocol-group packet-type]`). By default, flow detection automatically generates reports for events associated with the identification and tracking of culprit flows and bandwidth violations. Use commands at the **show ddos-protection** hierarchy level and **culprit-flows** or **culprit-flows detail** to display flow detection information and statistics on the basis of protocol, packet type, or subscriber management.

[See [DDoS Protection Flow Detection Overview](#)]

- **Excluding channel information from interface descriptions (MX Series)**—Starting in Junos OS Release 17.3R1, you can exclude channel information from being reported by default in the description for channelized interfaces that are included in RADIUS attributes such as NAS-Port-ID (87) and Calling-Station-ID (31). In earlier releases, you can exclude only adapter (PIC) and subinterface (logical interface number) information from an interface description.

[See [Interface Text Descriptions for Inclusion in RADIUS Attributes](#).]

- **BPCEF phase 2 enhancements (MX Series)**—Starting in Junos OS Release 17.3R1, support for additional OCS and PCRF features are added using Gy and Gx protocols. The new statements:
 - **accept-sdr** is added for PCRF partition at the `[edit access pcrf partition partition-name]` hierarchy level.
 - **alternative-diameter-partition** is added for OCS partition at the `[edit access ocs partition partition-name]` hierarchy level.

[See [Understanding Gx Interactions Between the Router and the PCRF](#) and [Configuring the Diameter Transport](#).]

- **System logs and traps added for Diameter peer connect/disconnect state changes (MX Series)**—Starting in Junos OS Release 17.3R1, the following event options related to Diameter peer connect and disconnect events are available to raise a trap when the corresponding state change occurs:
 - `jdiameterd_dne_state_connected`—Diameter network element (DNE) connected over a single peer.
 - `jdiameterd_dne_state_fully_connected`—DNE connected through at least two peers.
 - `jdiameterd_dne_state_disconnected`—DNE lost its connection.
 - `jdiameterd_peer_premiership_acquired`—Peer became primary for DNE.
 - `jdiameterd_peer_premiership_released`—Peer stopped being primary for DNE.
 - `jdiameterd_peer_state_down`—Peer is closing.
 - `jdiameterd_peer_state_open`—Peer reached i-open state.
 - `jdiameterd_peer_state_suspected`—Peer is downgraded to suspected state.

You can configure these at the `[edit event-options policy policy-name]` hierarchy level. Each of the event traps generates a corresponding ERRMSG system log.

[See [System Log Explorer](#).]

- **Diameter peers and transports support IPv6 addresses (MX Series)**—Starting in Junos OS Release 17.3R1, you can use IPv6 addresses for Diameter peers and transport connections. You must configure the same address family type for corresponding peers and transport connections. In earlier releases, only IPv4 addresses are supported, requiring the use of NAT to enable peering between IPv4 and IPv6 Diameter nodes.

[See [Configuring Diameter Peers](#) and [Configuring the Diameter Transport](#).]

- **Support for concurrent subscriber secure policy and FlowTapLite (MX Series)**—Starting in Junos OS Release 17.3R1, you can enable both DTCP-based flow-tap services on tunnel interfaces (FlowTapLite) and DTCP-initiated and RADIUS-initiated subscriber secure policies concurrently on the same router. Concurrent support enables using DTCP for monitoring both dynamic subscribers and static logical interfaces for business subscribers, as in a Layer 2-based wholesale topology that uses Extensible Subscriber Services Manager (ESSM). In earlier releases, concurrent use of subscriber secure policies and FlowTapLite is not supported.

[See [Guidelines for Configuring Subscriber Secure Policy Mirroring](#).]

- **Disabling RADIUS-initiated subscriber secure policy mirroring (MX Series)**—Starting in Junos OS Release 17.3R1, you can use the `dtcp-only` statement to prevent RADIUS-initiated subscriber secure policy mirroring from being enabled, while allowing both DTCP-initiated mirroring and DTCP-based flow-tap services (FlowTapLite) to be enabled. Requests from RADIUS to attach a subscriber secure policy (mirroring service) to a subscriber are rejected. This statement has no effect on existing RADIUS-initiated mirroring services. You must issue the statement before such services are activated for a subscriber. Subscriber login and session establishment are not affected.

[See [Disabling RADIUS-Initiated Subscriber Secure Policy Mirroring](#).]

- **Appending subscriber information to redirect URLs (MX Series)**—Starting in Junos OS Release 17.3R1, you can append information about the subscriber retrieved from the subscriber session database when the redirect URL is returned to the HTTP client. You specify the attributes in the redirect URL format in the Activate-Service VSA (26–65) or Deactivate-Service VSA (26–66) included in the RADIUS Access-Accept message when the subscriber is authenticated or in a Change of Authorization (CoA) message. Only the following attributes are supported: subscriber IP or IPv6 address, NAS IP address, requested URL, NAS port ID, MAC address, subscriber session ID, and username.

[See [Adding Subscriber Information to HTTP Redirect URL](#).]

- **HTTP status code 307 support (MX Series)**—Starting in Junos OS Release 17.3R1, the HTTP status code returned with the redirect URL by the redirect server depends on the HTTP version used by the HTTP client that sent the GET message. When the version is later than 1.0, the 307 (Temporary Redirect) status code is returned. When the version is 1.0, the 302 (Found) status code is returned. In earlier releases, only the 302 status code is returned with the redirect URL. Both codes inform the HTTP client to use the original URL for subsequent GET requests.

[See [HTTP Redirect Service Overview](#).]

- **Subscriber management support for Junos Node Slicing**—Starting with Junos OS Release 17.3R1, the MX Series routers that have Junos Node Slicing configured support all subscriber management features and services. Subscriber management provides capabilities such as subscriber access, authentication, and service creation, activation, and deactivation. The subscriber management services include DHCP, PPP, L2TP, VLAN, and pseudowire. However, in this release, the subscriber management services for Junos Node Slicing do not include advanced services and do not support unified in-service software upgrade (unified ISSU).
- **Support for Broadband Edge on MX10003 routers**—Starting in Junos OS Release 17.3R1, MX10003 supports the next-generation broadband edge software architecture for wireline subscriber management. With enhanced subscriber management, you can take advantage of optimized scaling and performance for configuration and management of dynamic interfaces and services for subscriber management.

Virtual Chassis

- **Support for host infrastructure(MX10003)**—Starting in Junos OS Release 17.3R1, MX10003 supports host infrastructure that can launch Junos OS virtual machine (VM) based on configuration data, monitor and manage the VM and the host-networking infrastructure, support Junos OS and host software upgrade, collect hardware errors for Junos OS error reporting and act as a proxy to Junos OS for executing host operations. Only one VM is supported per Routing Engine.

SEE ALSO

[Changes in Behavior and Syntax | 135](#)

[Known Behavior | 145](#)

[Known Issues | 154](#)

[Resolved Issues | 174](#)

[Documentation Updates | 214](#)

[Migration, Upgrade, and Downgrade Instructions | 215](#)

[Product Compatibility | 222](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [Class of Service | 136](#)
- [EVPNs | 136](#)
- [General Routing | 137](#)
- [High Availability \(HA\) and Resiliency | 138](#)
- [Infrastructure | 138](#)
- [Interfaces and Chassis | 138](#)
- [Management | 138](#)
- [MPLS | 139](#)
- [Network Management and Monitoring | 140](#)
- [Routing Protocols | 141](#)
- [Security | 142](#)
- [Services Application | 142](#)
- [Software Installation and Upgrade | 143](#)
- [Subscriber Management and Services | 143](#)
- [User Interface and Configuration | 144](#)
- [VLAN Infrastructure | 145](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 17.3R3 for MX Series routers.

Class of Service

- **Junos commit notification of unsupported configuration**—Junos OS does not support changing the **hierarchical-scheduler** mode of a logical tunnel interface, or redundant logical tunnel interface, if an active pseudowire subscriber interface is attached to it. A commit error has now been added to provide the notification.

EVPNs

- **commit check command successful with trunk port and EVPN-MPLS/EVPN-VXLAN EVI configured**—Starting in Junos OS Release 17.3R1, when adding a trunk port with dual tags to an EVPN and MPLS routing instance, or an EVPN and VXLAN routing instance, the CLI commit check configuration considers the **inner-vlan-id-list** statement and is successful.
- **Changes in the output of show route table command**—Starting in Junos OS Release 17.3R2, the output for **show route table** no longer displays the loopback address as the route distinguisher for MAC address virtual routing and forwarding (MAC-VRF) routing instances route entries. Instead, the output now displays the route distinguisher for the evpn and virtual switch instance type.
- **Support for LSP on EVPN-MPLS**—Starting in Junos OS Release 17.3R3, Junos supports the mapping of EVPN traffic to specific label-switched paths (LSPs). Prior to this release, the traffic policies mapping extended community to specific LSPs did not work properly.
- **Changes in the show route extensive output**—Starting in Junos OS Release 17.3R3, the output for **show route extensive** displays unknown evpn, opaque, and experimental extended communities as follows:
 - EVPN: unknown iana evpn Oxtype:Oxsubtype:Oxvalue
 - OPAQUE: unknown iana opaque Oxtype:Oxsubtype:Oxvalue
 - EXP: unknown Oxtype:Oxsub-type:Oxvalue

where type, sub-type, and value are defined in RFC 4360 *BGP Extended Communities Attribute*, RFC7153 *IANA Registries for BGP Extended Communities*. Internet Assigned Numbers Authority (IANA) maintains a registry with information on the type and subtype field values at

<https://www.iana.org/assignments/bgp-extended-communities/bgp-extended-communities.xhtml>

General Routing

- **MS-MPC and MS-MIC service package (MX240, MX480, MX960, MX2020, MX2010, and MX2008)**—PICs of the MS-MPC and MS-MIC do not support any service package other than extension-provider. If you try to configure any other service package for these PICs by using the **set chassis fpc slot-number pic pic-number adaptive-services service-package** command, an error is logged. Use the **show chassis pic fpc-slot slot pic-slot slot** command to view the service package details of the PICs.

[See [extension-provider](#).]

- **Change in boot up behavior (MX10003)**—Starting in Junos OS Release 17.3R1, when the MPC is removed and plugged into the slot, the MPC is brought online automatically. In Junos OS 17.3R1 prior releases, the MPC could be brought online only after issuing the **request chassis fpc slot number online** command.
- **Commit preparation on MX-VC setup**—On MX Series virtual chassis setup, you see the following:
 - When you issue **commit prepare** on one Routing Engine followed by switchover, the Routing Engine where the switchover command is issued reboots. Therefore, the prepared cache gets cleared in that Routing Engine.
 - **clear system commit prepared** clears the plus files and prepared cache only in the device where the command is issued.
- **Support for deletion of static routes when the BFD session goes down (MX Series)**—Starting with Junos OS Release 17.3R1, the default behavior of the static route at the **[edit routing-options static static-route bfd-admin-down]** hierarchy level is active. So, the static routes are deleted when the BFD receives a session down message.
- **Zero MAC address (00:00:00:00:00:00) treated as "my mac" (MX Series)**—When an Ethernet packet arrives in ingress, pre-classifier engine will perform a lookup of MAC address. If the MAC address matches an entry in the pre-classifier Ternary Content Addressable Memory (TCAM) and the entry has "my mac" attribute, pre-classifier engine will set the "my mac" bit in the cookie prepended to the incoming packet. In current implementation, MAC address "00:00:00:00:00:00" (zero MAC) is programmed as default value for "my mac" TCAM entries when the pre-allocated entries are not used or configured. Hence the packets with zero MAC are marked as "my mac" in the packet cookie. Forwarding engine will check "my mac" bit in the packet cookie. If "my mac" bit is 0, the packet will be dropped. If "my mac" bit is 1, further L2, L3, MPLS lookup will be performed. The "my mac" behavior is applicable since the day one release.

High Availability (HA) and Resiliency

- **Command 'show chassis in-service-upgrade' not available (MX10003)**—In this release, the command **show chassis in-service-upgrade** is not available for MX10003 routers. If you enter this command, the following output is shown: **error: command is not valid on the JNP10003 [MX10003]**. Earlier, the output shown for this command was **error: Unrecognized command (chassis-control)**.

Infrastructure

- **Change in support for interface-transmit-statistics statement (MX Series)**—You cannot configure aggregated Ethernet interfaces to capture and report the actual transmitted load statistics by using the **interface-transmit-statistics** statement. Aggregated Ethernet interfaces do not support reporting of the transmitted load statistics. The **interface-transmit-statistics** statement is not supported in the aggregated Ethernet interfaces hierarchy. In earlier releases, the **interface-transmit-statistics** statement was available in the aggregated Ethernet interfaces hierarchy but not supported.

Interfaces and Chassis

- **show chassis environment cb command not supported on MX10003 backup Routing Engine**—In Junos OS Release 17.3R1, you cannot get the environmental information about the Control Boards (CBs) installed in an MX10003 because the router does not support the **show chassis environment cb** CLI command on a backup Routing Engine. No output is displayed if you execute this command on an MX10003 backup Routing Engine.
- **Recovery of PICs that are stuck because of prolonged flow controls (MS-MIC, MS-MPC, MS-DPC, MS-PIC 100, MS-PIC 400, and MS-PIC 500)**—Starting in Junos OS Release 16.1R7, if interfaces on an MS-PIC, MS-MIC, MS-MPC, or MS-DPC are in stuck state because of prolonged flow control, Junos OS restarts the service PICs to recover them from this state. However, if you want the PICs to remain in stuck state until you manually restart the PICs, configure the new option **up-on-flow-control** for the **flow-control-options** statement at the **[edit interfaces mo-fpc/pic/port multiservice-options]** hierarchy level. In releases before Release 16.1R7, there is no action taken to recover service PICs from this state unless one of the options for the **flow-control-options** statement is configured, or service PIC is manually restarted.

Management

- **Changes to custom YANG RPC syntax (MX Series)**—Starting in Junos OS Release 17.3, custom YANG RPCs have the following changes in syntax:
 - The **junos:action-execute** statement is a substatement to **junos:command**. In earlier releases, the **action-execute** and **command** statements are placed at the same level, and the **command** statement is optional.

- The CLI formatting for a custom RPC is defined within the **junos-odl:format** statement, which takes an identifier as an argument. In earlier releases, the CLI formatting is defined using a container that includes the **junos-odl:cli-format** statement with no identifier.
- The **junos-odl:style** statement defines the formatting for different styles within the statement. In earlier releases, the CLI formatting for different styles is defined using a container that includes the **junos-odl:cli-format** and **junos-odl:style** statements.
- **Enhancement to show agent sensors command (MX Series)**—Starting with Junos OS Release 17.3R1, the **show agent sensors** command, which displays information about Junos Telemetry Interface sensors, displays the default value of **0** for the **DSCP** and **Forwarding-class** values. Previously, the displayed default value for these fields was **255**. The default value is displayed when you do not configure a DSCP or forwarding-class value for a sensor at the **[edit services analytics export-profile profile-name]** hierarchy level.

[See [export-profile](#) and [show agent sensors](#).]

MPLS

- Starting in Junos OS Release 17.3R1, the previously hidden configuration statement, **session**, can be configured at the **[edit protocols ldp]** hierarchy level. This statement enables you to configure the LDP session parameters by specifying the session destination address.

[See [session](#).]

- **Support for inet.0 and inet.3 labeled unicast BGP route for protocol LDP (MX Series)**--- Starting in Junos OS Release 17.3R3, LDP egress policy is supported on both inet.0 and inet.3 routing Information bases (RIBs) also known as routing table for labeled unicast BGP routes. If a routing policy is configured with a specific (inet.0 and inet.3) RIB, the egress policy is applied on the specified RIB. If no RIB is specified and a prefix is present on both inet.0 and inet.3 RIBs for labeled unicast BGP routes, then inet.3 RIB is preferred. However, prior to Junos OS Release 12.3R1 and starting with Junos OS Release 16.1R1, LDP egress policy is always preferred on inet.0 RIB and support for inet.3 RIB egress policy for labeled unicast BGP routes was disabled. In Junos OS Release 12.3R1 and later releases up to Junos Release 16.1R1, LDP egress policy was supported in inet.3 RIBs, in addition to inet.0 RIBs, for labeled-unicast BGP routes.
- **Disable M-LDP from using RSVP-TE LSPs for tunneling**—Starting in Junos OS Release 12.3R1, Junos OS provides support for Multipoint LDP (M-LDP) for Targeted LDP (T-LDP) sessions with unicast replication, in addition to link sessions. As a result, the current default behavior of M-LDP over RSVP tunneling is similar to unicast LDP.

However, because T-LDP is chosen over LDP and link sessions to signal point-to-multipoint LSPs, you can enable LDP natively throughout the network, so the point-to-multipoint LSPs take the LDP paths.

[See [p2mp \(Protocols LDP\)](#).]

- Starting in Junos OS Release 17.3R2-S2, the * (asterisk) wildcard character is supported for the interface name of the **show ppp interfaces** command for debugging purpose. With this support, you can match

any string of characters in that position in the interface name. For example, `so*` matches all SONET/SDH interfaces.

[See [show ppp interface](#).]

- **Loss of traffic over bypass MPLS LSPs**—If RSVP link or node protection is enabled along with global RSVP authentication, there is loss of traffic over bypass MPLS LSPs at the time of local repair, when the point of local repair (PLR) and the merge point devices have different versions of the Junos OS software installed on them. That is, one device is running a release prior to Junos OS Release 16.1, and the other device is running a release starting with Junos OS Release 16.1R4-S12.

Network Management and Monitoring

- **Enhancement to SNMPv3 traps for contextName field (MX Series)**—Starting in Junos OS Release 17.3R1, the contextName field in SNMPv3 traps generated from a non-default routing instance, is populated with the same routing-instance information as is given in SNMPv2 traps. SNMPv2 traps provide the routing-instance information as context in the form of context@community. This information gives the network monitoring system (NMS) the origin of the trap, which is information it might need. But in SNMPv3, until now, the contextName field was empty. For traps originating from a default routing instance, this field is still empty, which now indicates that the origin of the trap is the default routing instance.
- **Enhancement to about-to-expire logic for license expiry syslog messages (MX Series)**—Starting in Junos OS Release 17.3R1, the logic for multiple capacity type licenses and when their expiry raises alarms was changed. Previously, the behavior had alarms and syslog messages for expiring licenses raised based on the highest validity, which would mislead users in the case of a license expiring earlier than the highest validity license. The new behavior has the about-to-expire logic based on the first expiring license.
- **SNMP syslog messages changed (MX Series)**—In Junos OS Release 17.3R1, two misleading SNMP syslog messages have been rewritten to accurately describe the event:
 - OLD --AgentX master agent failed to respond to ping. Attempting to re-register
NEW -- AgentX master agent failed to respond to ping, triggering cleanup!
 - OLD -- NET-SNMP version %s AgentX subagent connected
NEW --- NET-SNMP version %s AgentX subagent Open-Sent!

[See the [MIB Explorer](#).]

- **Change in default log level setting (MX Series)**—In Junos OS Release 17.3R2, the following changes were made in default logging levels:

Before this change:

- SNMP_TRAP_LINK_UP was LOG_INFO for both the physical (IFD) and logical (IFL) interfaces.
- SNMP_TRAP_LINK_DOWN was LOG_WARNING for both the physical (IFD) and logical (IFL) interfaces.

After this change:

- IFD LinkUp -> LOG_NOTICE (since this is an important message but less frequent)
- IFL LinkUp -> LOG_INFO (no change)
- IFD and IFL LinkDown -> LOG_WARNING (no change)

[See the [MIB Explorer](#).]

- **Customer-visible SNMP trap name changes (MX Series)**—In Junos OS Release 17.3R2, on the Enhanced Switch Control Board (SCBE), name changes include the control board slot when `jnxTimingFaultLOSset` and `jnxTimingFaultLOSClear` traps are generated in the case of BITS interfaces (T1 or E1). SNMP traps for the backup Routing Engine clock failure event have been added, and the control board name is included in the SNMP trap interface name (`jnxClksyncIntfName`), for example, value: "external(cb-0)".

[See [SNMP MIB Explorer](#).]

- **New context-oid option for trap-options configuration statement to distinguish the traps which come from a non-default routing instance and non-default logical system (MX Series)**—In Junos OS Release 17.3R3, a new option, **context-oid**, for the **trap-options** statement allows you to handle prefixes such as `<routing-instance name>@<trap-group>` or `<logical-system name>/<routing-instance name>@<trap-group>` as an additional varbind.

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

- A decrease in the MPLS label-switched path (LSP) statistics pauses the SNMP MIB `mplsLspInfoAggrOctets` count for one MPLS statistics gathering interval. In such cases, the `mplsLspInfoAggrOctets` value is updated only after completing one more interval of the MPLS statistics gathering.

Routing Protocols

- **Change in the default behavior of advertise-from-main-vpn-tables configuration statement**—BGP now advertises EVPN routes from the main `bgp.evpn.0` table. You can no longer configure BGP to advertise the EVPN routes from the routing instance table. In earlier Junos OS Releases, BGP advertised EVPN routes from the routing instance table by default.

[See [advertise-from-main-vpn-tables](#).]

- **Change in output of show configuration routing-options flow operational command**—Starting in Junos OS Release 17.3R1, the sequence of statements in the output of **show configuration routing-options flow** operational command has changed to improve readability. The **then** statements are now displayed after the **match** conditions in a logical sequence.

- **BGP GR stale routes are not removed when BFD goes down**—Starting in Junos OS Release 17.3R1, 17.2R2, 17.1R3, 16.2R3, 16.1R5, and 15.1R7, when a BGP session that has BFD configured without the **hold-down-interval** fails, the BFD session remains active. The BFD session is not impacted even when graceful restart is enabled. BGP deletes the BFD session when user explicitly disables BFD on a BGP peer. Note that BFD session is created only when a BGP session is **Established**. In earlier Junos OS releases, BFD sessions are deleted when the BGP session fails and the **hold-down-interval** option is not configured.

Security

- **Support for SSH protocol version 2**—Starting in Junos OS Release 17.3R2, SSH protocol version 1 (SSHv1) is not supported. SSH protocol version 2 (SSHv2) is the default protocol-version option available under the `[edit system services ssh]` hierarchy level.

[See [protocol-version](#)]

Services Application

- **Changes to the show services rpm history-results command (MX Series)**—Starting in Junos OS Release 17.3R1, you must include the **owner** *owner* and **test** *name* options when using the **show services rpm history-results** command.

[See [show services rpm history-results](#).]

- In Junos OS Release 17.3R1 and later, for PIC-based J-Flow on MX Series routers and inline J-Flow on PTX Series routers, the Options template and Options data records include the **Sampling Interval** field as part of the **ScopeTemplate** field instead of the **ScopeSystem** field.

Software Installation and Upgrade

- **ZTP is supported on MX PPC platforms (MX Series)**—Starting in Junos OS Release 17.3R3, zero touch provisioning (ZTP) is supported on MX PPC platforms (which are MX5, MX10, MX40, MX80, and MX104 routers). Before the fix, the ZTP process did not start to load image and configuration for MX PPC routers.

[See [Junos OS Installation Package Names](#).]

Subscriber Management and Services

- **Source-specific multicast (SSM) CLI changes for dynamic IGMP and dynamic MLD (MX Series)**—Starting in Junos OS Release 17.3R1, the **ssm-map ssm-map-name** statement at the **[edit dynamic-profiles profile-name protocols (igmp | mld) interface interface-name]** hierarchy level is deprecated and does not appear in the CLI. Instead, you define an SSM map policy with the **policy-statement** statement at the **[edit policy-options]** hierarchy level. Apply the policy for dynamic IGMP or dynamic MLD with the **ssm-map-policy ssm-map-policy-name** statement at the **[edit dynamic-profiles profile-name protocols (igmp | mld) interface interface-name]** hierarchy level.

Before you upgrade from an earlier release with a configuration that includes **ssm-map**, delete the **ssm-map** statement. If you do not, the upgrade fails. If you perform the upgrade without validation (**no-validate**), the upgrade passes and the **ssm-map** configuration is accepted, but it has no effect.

[See [ssm-map-policy \(Dynamic IGMP Interface\)](#) and [ssm-map-policy \(Dynamic MLD Interface\)](#).]

- **Memory mapping statement removed for Enhanced Subscriber Management (MX Series)**—Starting in Junos OS Release 17.3R1, use the following command when configuring database memory for Enhanced Subscriber Management:

set system configuration-database max-db-size

CLI support for the **set configuration-database virtual-memory-mapping process-set subscriber-management** command has been removed to avoid confusion. Using the command for subscriber management now results in the following error message:

WARNING: system configuration-database virtual-memory-mapping not supported. error: configuration check-out failed.

[See [Interface Configuring Junos OS Enhanced Subscriber Management](#) for an example of how to use the **max-db-size** command.]

- **Change to ICRQ message inclusion of the ANCP Access Line Type AVP (MX Series)**—Starting in Junos OS Release 17.3R2, the ICRQ message includes the ANCP Access Line Type AVP (145) when the received ANCP Port Up message includes a DSL-type of 0 (OTHER). In earlier releases, the AVP is not sent when the value is 0.
- **Support for IPv6 all-routers address in nondefault routing instance (MX Series)**—Starting in Junos OS Release 17.3R3, the well-known IPv6 all-routers multicast address, FF02::2, is supported in nondefault

routing instances. In earlier releases it is supported only for the default routing instance; consequently IPv6 router solicitation packets are dropped in nondefault routing instances.

- **Correction to CLI for L2TP tunnel keepalives (MX Series)**—Starting in Junos OS Release 17.3R3, the CLI correctly limits to 3600 seconds the maximum duration that you can enter for the hello interval of an L2TP tunnel group. In earlier releases, the CLI allows you to enter a value up to 65,535, even though only 3600 is supported.

See [hello-interval \(L2TP\)](#).

- **Wildcard supported for show subscribers agent-circuit-identifier command (MX Series)**—Starting in Junos OS Release 17.3R3, you can specify either the complete ACI string or a substring when you issue the **show subscribers agent-circuit-identifier** command. To specify a substring, you must enter characters that form the beginning of the string, followed by an asterisk (*) as a wildcard to substitute for the remainder of the string. The wildcard can be used only at the end of the specified substring; for example:

```
user@host1> show subscribers agent-circuit-identifier substring*
```

In earlier releases, starting with Junos OS Release 14.1, the command requires you to specify the complete ACI string to display the correct results. In Junos OS Release 13.3, you can successfully specify a substring of the ACI without a wildcard.

- **Changed behavior for framed routes without a subnet mask (MX Series)**—Starting in Junos OS Release 17.3R3, the router connects the session but ignores a framed route when it is received from RADIUS in the Framed-Route attribute (22) without a subnet mask.

In earlier releases, the router installs the framed route with a Class A, B, or C subnet mask depending on the value of the first octet. When the octet < 128, the mask is /8; when 128 <= octet < 192, the mask is /16; and when the octet >= 192, the mask is 24.

- **Bandwidth options match for inline services and tunnel services (MX Series)**—Starting in Junos OS Release 17.3R3, you can configure the same bandwidth options for inline services with the **bandwidth** statement at the **[edit chassis fpc slot-number pic number inline-services]** hierarchy level as you can configure for tunnel services with the **bandwidth** statement at the **[edit chassis fpc slot-number pic number tunnel-services]** hierarchy level.

[See [bandwidth \(Inline Services\)](#) and [bandwidth \(Tunnel Services\)](#)]

User Interface and Configuration

- Starting in Junos OS Release 17.3R3, the delegate probes are distributed evenly across the interval of 3 seconds to avoid the packet bursts in the network due to real-time performance monitoring (RPM). RPM syslogs are processed with the increase in the ramp up time of RPM delegates tests to 60 seconds. With RPM syslogs processed, the chances of multiple tests starting and ending at the same time are smaller, thus a potential restriction in **event-processing**.

- **Junos OS prohibits configuring ephemeral configuration database instances that use the name default (MX Series)**—Starting in Junos OS Release 17.3R3, user-defined instances of the ephemeral configuration databases, which are configured using the **instance *instance-name*** statement at the **[edit system configuration-database ephemeral]** hierarchy level, do not support configuring the name **default**.

VLAN Infrastructure

- **LAG interface flaps while adding/removing a VLAN**—From Junos OS Release 17.3 or later, the LAG interface flaps while adding or removing a VLAN. The flapping happens when a low-speed SFP is plugged into a relatively high-speed port. To avoid flapping, configure the port speed to match the speed of the SFP.

SEE ALSO

[New and Changed Features | 103](#)

[Known Behavior | 145](#)

[Known Issues | 154](#)

[Resolved Issues | 174](#)

[Documentation Updates | 214](#)

[Migration, Upgrade, and Downgrade Instructions | 215](#)

[Product Compatibility | 222](#)

Known Behavior

IN THIS SECTION

- [Class of Service \(CoS\) | 146](#)
- [EVPN | 146](#)
- [Forwarding and Sampling | 148](#)
- [General Routing | 148](#)
- [High Availability \(HA\) and Resiliency | 150](#)
- [Infrastructure | 150](#)
- [Interfaces and Chassis | 151](#)
- [MPLS | 151](#)

- Platform and Infrastructure | 152
- Routing Protocols | 152
- Services Application | 152
- Software Installation and Upgrade | 153
- Subscriber Management and Services | 153

This section contains the known behavior, system maximums, and limitations in hardware and software in Junos OS Release 17.3R3 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)

- In Junos OS Release 17.2, egress rate limit at the extended port does not work properly when you have a rate-limit configuration applied at the extended port physical interface (IFD) level by **traffic-control-profile-remaining** and also at some of the extended port logical interfaces (IFL) by **explicit traffic-control-profile** in hierarchical-scheduler mode. [PR1271719](#)

EVPN

- Routing instances of type EVPN configured with a VLAN ID will advertise MAC (type 2) routes with the VLAN value in the Ethernet tag field of the MAC route. As a workaround, use **vlan-id-none** to claim the RFC compliance. [PR945247](#)
- A provider edge (PE) device running EVPN IRB with an IGP configured in a VRF associated with the EVPN instance will be unable to establish an IGP adjacency with a CE device attached to a remote PE device. The IGP instance running in the VRF on the PE device might be able to discover the IGP instance running on the remote CE device through broadcast or multicast traffic, but will be unable to send unicast traffic directly to the remote CE device. [PR977945](#)
- In scaled up EVPN VPWS configurations (approximately 8000 EVPN VPWS), during Routing Engine switchover, rpd scheduler slip messages might be seen. [PR1225153](#)
- Configurable udp-port for VXLAN in EVPN-VXLAN scenario is currently not supported. [PR1249310](#)
- On an MX Series router running Junos OS, while migrating a routing instance from VPLS to EVPN, if an EVPN command (for example, **control-word**) is handled in a catastrophic manner by daemons (processes), traffic loss can occur while the control plane state is cleaned up and reconstructed. [PR1268428](#)

- In a hub-and-spoke VPLS environment running Junos OS, if local switching is enabled on the hub-and-spoke PE devices migrated to EVPN (for which the hub remains VPLS-only), the following issue could occur: (1) Two copies of BUM traffic could be received at the spoke PE device (one copy through the EVPN next hop from the ingress spoke and the other copy through the VPLS pseudowire from the hub) and (2) MACs behind a spoke PE device would use the VPLS pseudowire to the hub as the next hop on the remote spoke PE devices (instead of the EVPN next hop). This issue occurs because the VPLS-only hub continues to provide an alternative forwarding path between the spoke PE devices (migrated to EVPN). [PR1272449](#)
- An IPv6 underlay with an IPv6 overlay with IRB is not supported in a bridge domain, because having two IPv6 headers exceeds the 128-byte parcel size for the line card. [PR1274709](#)
- In an EVPN network with VXLAN encapsulation configured for direct-nexthop mode ("pure type 5" mode without overlay gateway addresses), at least one type 5 route per VRF from a remote endpoint must be received and installed in the local routing table of a device, to enable the local device to forward inbound type 5 traffic received from the remote endpoint. If the local device has not installed at least one route with a next hop pointing toward a specific remote endpoint, type 5 VXLAN-encapsulated IP traffic sent by the remote endpoint toward the local device will not be forwarded correctly. [PR1305068](#)
- When changing encapsulation from VXLAN to MPLS or vice versa, you need to deactivate and reactivate the instance. [PR1326430](#)
- When the vxlan VNI is removed at remote PE device, the flood groups are cleaned up and the MAC routes are deleted. The router continues to accept traffic for the duration the remote node sends traffic to the VNI that is cleaned up. The show commands will reflect the VNI as valid until the tunnel to the remote PE device is deleted. No operational impact. [PR1366983](#)
- When moving MACs between single or multi-homed locations in rapid succession, it is possible that some MACs might experience a delay before converging to the final expected state. This is due to the absence of the MAC mobility sequence number in Junos OS Release 17.4R1 and earlier releases. Mobility sequence number support in Junos OS Release 17.4R1 and later allows MAC moves to converge rapidly and deterministically. [PR1369234](#)

Forwarding and Sampling

- Loopback filters: All counters associated with RE PROTECT IPv4 & IPv6 Filter are not getting cleared after deactivating its binding from Lo0 interface. [PR1230761](#)

General Routing

- On MX Series routers, parity memory errors occur in the pre-classifier engines within an MPC. Packets silently discarded earlier are reported in syslogs and alarms when parity memory errors occur.
- On an MX10003 router, when the management interface (fxp0 or em0) is down on the master Routing Engine, in addition to the **Ethernet Link Down** alarm, an additional **Management Ethernet Link Down** alarm is also raised.
- A provider edge (PE) device running EVPN IRB with an IGP configured in a VRF associated with the EVPN instance will be unable to establish an IGP adjacency with a CE device attached to a remote PE device. The IGP instance running in the VRF on the PE device might be able to discover the IGP instance running on the remote CE device through broadcast or multicast traffic, but will be unable to send unicast traffic directly to the remote CE device. [PR977945](#)
- On MX Series routers with MS-MPC or MS-MIC, memory leaks will be seen with jnx_msp_jbuf_small_oc object, upon sending millions of point-to-point tunneling protocol control connections (3-5M) alone at higher cells per second (cps) (greater than 150K cps). This issue is not seen with up to 50,000 control connections at 10,000-30,000 cps. [PR1087561](#)
- NAT64: Source-prefix filtering and protocol filtering of the CGNAT sessions are incorrect. For example, **show services sessions extensive protocol udp source-prefix <0:7000::2>** displays incorrect filtering of the sessions. [PR1179922](#)
- Chef for Junos OS supports additional resources to enable easier configuration of networking devices. These are available in the form of netdev-resources. The netdev-resource developed for interface configuration has a limitation to configure the XE interface. Netdev-interface resource assumes that speed is a configurable parameter that is supported on a GE interface but not on an XE interface. Hence, netdev-interface resource cannot be used to configure an XE interface due to this limitation. This limitation is applicable to packages chef-11.10.4_1.1.*.tgz chef-11.10.4_2.0.*.tgz in all platforms {i386/x86-32/powerpc}. [PR1181475](#)
- As described in RFC 7130, when LACP is used and considers the member link to be ready to forward traffic, the member link must not be used by the load balancer until all the micro-BFD sessions of the particular member link are in the up state. [PR1192161](#)
- In certain interface scaling scenarios, during configuration commit/rollback, you might see an fpcx error message. You can safely ignore this message because of the FPGA monitor mechanism on DPC cards for logical interface mapping (ifl_map). Between the deletion of a physical interface and the monitoring event, this mechanism checks through the stored logical interfaces. While the mechanism tries to find

the family of a recently deleted logical interface that was not cleaned from the the ifl_map, harmless messages might populate the log file. [PR1210877](#)

- The ptp master streams on IP and Ethernet are not supported simultaneously. [PR1217427](#)
- There is no unified ISSU from Junos OS Release 15.1 and earlier releases to Junos OS Release 16.2R1. [PR1222540](#)
- The following MICs in MPC2E-NG/MPC3E-NG are non PHY-Timestamping capable: MIC-3D-4XGE-XFP MIC3-3D-10XGE-SFPP, MIC-3D-2XGE-XFP, MIC-3D-20GE-SFP. The 2Way/T1/T4 time error can be up to +/-450 nsec in these MICs. [PR1243646](#)
- When some route next hop has been created by the application, it is assumed that it can propagate to the rest of the system. KRT asynchronously picks up this state for propagation. There is no reverse indication to the application, if there was an error in propagating the state. The system is supposed to eventually reconcile. So, if SPRING-TE produces a <route> pair that looks legal from the application standpoint, but KRT is not able to download it to the kernel, because kernel rejected the next hop, the <route> sort of get stuck in routing protocol process (rpd). In the meantime, the previous version of the route (L-ISIS in this case) that was downloaded still lingers in the kernel and Packet Forwarding Engine. [PR1253778](#)
- 1PPS TE/cTE performance metric can be as high as +/-550 nsec in MPC2E/3E NG QoS/3D 20x 1GE(LAN)-E,SFP with no PHY-timestamp and non-hybrid mode. [PR1263235](#)
- This issue occurs when an interface comes online and both the OAM protocol and MKA protocol try to establish their respective sessions. Because of contention between these two protocols OAM takes down the interface and MKA fails to establishes a connection (because the interface is down, it cannot send out MKA packets). [PR1265352](#)
- PCC controlled LSP metric not getting updated on the controller, PCE-delegated LSPs do not come up. [PR1265864](#)
- On an MX Series router running Junos OS, while migrating a routing instance from VPLS to EVPN, if an EVPN command (for example, control-word) is handled in a catastrophic manner by daemons (processes), traffic loss can occur while the control plane state is cleaned up and reconstructed. [PR1268428](#)
- In a hub-and-spoke VPLS environment running Junos OS, if local switching is enabled on the hub-and-spoke PE devices migrated to EVPN (for which the hub remains VPLS-only), the following issue could occur: (1) Two copies of BUM traffic could be received at the spoke PE device (one copy through the EVPN next hop from the ingress spoke and the other copy through the VPLS pseudowire from the hub) and (2) MACs behind a spoke PE device would use the VPLS pseudowire to the hub as the next hop on the remote spoke PE devices (instead of the EVPN next hop). This issue occurs because the VPLS-only hub continues to provide an alternative forwarding path between the spoke PE devices (migrated to EVPN). [PR1272449](#)
- The device might not power up when crossover cables are used. We recommend using straight cables. [PR1274613](#)

- An IPv6 underlay with an IPv6 overlay with IRB is not supported in a bridge domain, because having two IPv6 headers exceeds the 128-byte parcel size for the line card. [PR1274709](#)
- On MX104 **JTASK_SCHED_SLIP** seen on committing randomly. [PR1281016](#)
- On MX150 routers, if you connect an even-numbered port to another even-numbered port using external loopback, they cannot communicate with each other. On MX150 routers, **ge-0/0/0,2,4,6,8,10** and **xe-0/0/12** are identified as even-numbered ports. Also, if you connect an odd-numbered port to another odd-numbered port using external loopback, they cannot communicate with each other. On MX150 routers, **ge-0/0/1,3,5,7,9,11** and **xe-0/0/13** are identified as odd-numbered ports.

For instance, if you connect port (**ge-0/0/0**) to port (**ge-0/0/6**) using external loopback, the two ports cannot communicate with each other. Also, if you connect port (**ge-0/0/3**) to port (**ge-0/0/9**) using external loopback, the two ports cannot communicate with each other. To configure external loopback, connect an even-numbered port (for instance, **xe-0/0/12**) to an odd-numbered port (for instance, **xe-0/0/13**).

- Asymmetric cipher-suite configuration with aes256 and aes256-xpn on MACSec peer nodes mka session comes up. [PR1332156](#)

High Availability (HA) and Resiliency

- **MPC7E MPC8E and MPC9E line card restrictions for MX Series Virtual Chassis unified ISSU (MX Series)**—MPC7E, MPC8E, and MPC9E line cards do not support unified ISSU in Junos OS Release 17.3R1 for MX Series Virtual Chassis configurations. These line cards must be removed or configured to power off during the MX-VC ISSU process. ISSU in Junos OS Release 17.3R1 is supported for MX Series standalone chassis configurations.

[See [Preparing for a Unified ISSU in an MX Series Virtual Chassis](#).]

Infrastructure

- Executing a **restart chassisd** in a MX Series Virtual Chassis router with the following elements configured might result in generating a core file.
 - IGP - OSPF/OSPF3 (area 0, LFA) IS-IS (level 2, LFA) LDP synchronization IPv4 and IPv6.
 - IBGP - dual, redundant route reflection IPv4 and IPv6.
 - MPLS - LDP (IGP synchronization, track IGP metric) RSVP (node link protection, adaptive, auto bandwidth, refresh reduction).
 - L3VPN OSPF, OSPF3, BGPv4, BGPv6, RIPv2, static, MBGP, NGEN-MVPN, l3vpn cnh with ext space, any to any, hub and spoke, MPLS access, Ethernet access, multicast extranet, per VPN and per prefix labels, SRX-based network address translation, SRX-based firewall.
 - Direct Internet Access - EBGP.

- CoS - BA/MF classification, policing or shaping, queuing or scheduling, hierarchical queuing, shaping, or scheduling, 8 traffic classes.
- BFD, OAM, or CFM - liveness detection.
- Load Balancing - L2 aggregate Ethernet, IP equal cost multi path, MPLS equal cost multi path.
- High Availability - GRES/NSR, ISSU, fabric redundancy, tail end protection, BGP prefix independent convergence edge.
- Security - loopback filter, arp policers, control plane traffic policers, urpf check with all feasible paths, TTL filtering, J-Flow or ipfix export only, SRX based DDOS. [PR1352227](#)

Interfaces and Chassis

- Previously, the same IP address could be configured on different logical interfaces from different physical interfaces in the same routing instance (including master routing instance), but only one logical interface is assigned with the identical address after commit. There is no warning during the commit, only syslog messages indicating incorrect configuration. This issue is fixed and it is now not allowed to configure the same IP address (the length of the mask does not matter) on different logical interfaces. [PR1221993](#)
- Convergence time for VRRP traffic is higher when the router or Routing Engine is rebooted in a single Routing Engine system. We recommend having a dual Routing Engine system with redundancy enabled. In this case, if the master Routing Engine is rebooted, the backup Routing Engine will take over mastership. There will not be any disruption in VRRP traffic. [PR1270168](#)
- When an FPC with both core link and member link of an aggregated Ethernet interface (running VRRP) is restarted or offlined, the convergence time will be higher. [PR1270811](#)
- Higher MTU configuration on an IRB than on the member link of its VLAN might bring down a VRRP session configured on the IRB. As a workaround, always have the MTU configured on the IRB of the VLAN be less than or equal to the MTU configured on its member links of the same VLAN because MX Series devices do not throw error or warning messages during configuration commit. [PR1295763](#)
- In subscriber management scenario with PPPoE access models, during a unified ISSU, it is possible to lose a small number of active subscribers after the unified ISSU is completed if certain timing conditions occur. These timing conditions might trigger session database related discrepancies between the jpppd daemon and the underlying statesync infrastructure causing the subscriber record loss. These subscribers, however, should be able reconnect right away minimizing any service outage. [PR1360870](#)

MPLS

- It takes longer to set-up L3 vpn egress protection starting from JUNOS version 16.1R1. [PR1278535](#)
- When NG-MVPN is configured with RSVP provider tunnels and NSR is used, then the egress router for the tunnel might not correctly replicate some of the tunnel state to the backup routing engine, leading to temporary traffic loss during NSR failover for the affected tunnels. [PR1293014](#)

- In Junos OS Release 17.1R1 or earlier releases, labels from within the following ranges can be used as incoming labels for static VPLS LSI-based services by default: R1. [29696 - 41983]; R2. [1000000 - 1048575]. In Junos OS Release 17.1R1 and later releases on a system operating in enhanced-IP mode, range R1 cannot be used any longer for static VPLS LSI-based services incoming label assignment by default. This limitation is applicable only for range R1 and is not applicable for range R2. The latter works on Junos OS Release 17.1R1 and later releases just as it does on previous Junos OS releases. [PR1307402](#)

Platform and Infrastructure

- Oct 18 10:34:10 jtac-mx480-r2043 jlaunchd: commit-batch is thrashing, not restarted [PR1284271](#)

Routing Protocols

- When a Junos OS aggregation gateway uses a IPv6 address as next hop for IPv4 aggregates announced to downstream, it might attract traffic prematurely before Packet Forwarding Engines are programmed with more specific IPv4 routes. This happens when the IPv6 address is advertised in BGP inet6-labeled-unicast family. [PR1220235](#)
- PIM is not supported on a tunnel interface configured with an inet6 address. Configuring PIM over a tunnel interface with an inet6 address might cause the routing protocol process (rpd) to crash and generate a core file. [PR1267570](#)
- In MX80 (unlike other MX Series), ospf spring is not supported. [PR1272991](#)

Services Application

- Account Session ID, Interface Identifier, and Subscriber User Name trigger attributes are optimized for a scaled subscriber management environment. If you include any of the other, non-optimized, trigger attributes in a scaled subscriber management environment, a significant delay might be observed between the time when the DTCP ADD message is sent and the time when forwarding starts for the mirrored traffic. For example, if there are 10,000 subscriber sessions on the router, forwarding of the mirrored traffic might be delayed for 20 minutes. This delay occurs when you specify any non-optimized attribute, with or without any optimized attribute. The delay occurs regardless of the order of attributes in the DTCP packet. [PR1269770](#)
- Broadband-edge platforms do not support service-set integration with dynamic profiles when the service set is representing a carrier-grade NAT configuration. As a workaround, you can use next-hop service set configurations and routing options to steer traffic to a multiservices (ms) interface where NAT functionality can be exercised. The following configuration snippet shows the basics of statically configuring the multiservices interface next hop and a next-hop service set. Traffic on which the service is applied is forced to the interface inside the network by configuring that interface as the next hop. This configuration does not show other routing-options or NAT configurations relevant to your network.


```

routing-options {
  static {
    route 0.0.0.0/0 {
      next-hop ms-3/0/0.1;
      preference 0;
    }
  }
  ...
}
services {
  service-set CGN {
    nat-rules CGN_SAMPLE;
    next-hop-service {
      inside-service-interface ms-3/0/0.1;
      outside-service-interface ms-3/0/0.2;
    }
  }
  nat {
    ...
  }
}

```

[See [Configuring Service Sets to be Applied to Services Interfaces.](#)]

Software Installation and Upgrade

- **Unified ISSU with active BBE subscribers using advanced services supported only to 17.3R3 and later 17.3 releases**—If you have active broadband edge subscribers that are using advanced services, you cannot perform a successful unified in-service software upgrade (ISSU) to a Junos OS 17.3 release earlier than 17.3R3. If you perform an ISSU to a 17.3 release earlier than 17.3R3, the advanced services PCC rules are not attached to subscribers.
- **Unified ISSU not supported with an active RPM configuration**—If you have an active real-time performance monitoring (RPM) configuration, you cannot perform a successful unified in-service software upgrade (ISSU) to a Junos OS 17.3 release. The warning **ISSU is not supported for RPM configuration** appears.

Subscriber Management and Services

- The **all** option is not intended to be used as a means to perform a bulk logout of L2TP subscribers. We recommend that you do not use the **all** option with the **clear services l2tp destination**, **clear services l2tp session**, or **clear services l2tp tunnel** statements in a production environment. Instead of clearing

all subscribers at once, consider clearing subscribers in smaller group, based on interface, tunnel, or destination end point.

- Before you make any changes to the underlying interface for a demux0 interface, you must ensure that no subscribers are currently present on that underlying interface. If any subscribers are present, you must remove them before you make changes.

SEE ALSO

[New and Changed Features | 103](#)

[Changes in Behavior and Syntax | 135](#)

[Known Issues | 154](#)

[Resolved Issues | 174](#)

[Documentation Updates | 214](#)

[Migration, Upgrade, and Downgrade Instructions | 215](#)

[Product Compatibility | 222](#)

Known Issues

IN THIS SECTION

- [Class of Service \(CoS\) | 155](#)
- [EVPN | 155](#)
- [Forwarding and Sampling | 157](#)
- [General Routing | 158](#)
- [High Availability \(HA\) and Resiliency | 164](#)
- [Infrastructure | 165](#)
- [Interfaces and Chassis | 165](#)
- [Layer 2 Ethernet Services | 166](#)
- [Layer 2 Features | 167](#)
- [MPLS | 167](#)
- [Platform and Infrastructure | 168](#)
- [Routing Protocols | 170](#)
- [Services Applications | 172](#)

- [Subscriber Access Management | 172](#)
- [User Interface and Configuration | 173](#)
- [VPNs | 173](#)

This section lists the known issues in hardware and software in Junos OS Release 17.3R3 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)

- A CoS scheduler update might fail when all of the following conditions are met:
 - Dynamic subscribers exist on an aggregated Ethernet bundle.
 - CoS traffic-control-profile or scheduler-map (or both) applied to these dynamic subscribers is from a static configuration.
 - The relevant static CoS is modified in the same configuration commit as a modification to the aggregated Ethernet bundle (either a leg add or leg remove) containing the subscribers.
 - The leg add or leg remove in the commit is the first or last leg to be added or removed from a line card.

In this event, one of the following logs is displayed in the message system log: **subscriber cos update not applied to interface <interface-name> status <id>** or **subscriber cos update not applied to interface-set <interface-set-name> status <id>**. These messages indicate that the last update to the subscriber or interface set was not applied. As a workaround, remove the last CoS update, commit the configuration, reapply the CoS update, and commit the configuration. [PR1276459](#)

EVPN

- The Layer 2 address learning process (l2-ald) might generate a core file in a scaled L2 setup, including bridge domain, VPLS, EVPN, and so on. The l2-ald core file usually follows a kernel page fault that recovers on its own. In some cases, a manual restart of the process is needed to recover logs: **/kernel: %KERN-3-BAD_PAGE_FAULT: pid 69719 (l2ald), uid 0: pc 0x88beb5ce got a read fault at 0x6ca, x86 fault flags = 0x4 /kernel: %KERN-6: pid 69719 (l2ald), uid 0: exited on signal 11 (core dumped) init: %AUTH-3: l2-learning (PID 69719) terminated by signal number 11.** A core file is generated. [PR1142719](#)
- In an EVPN scenario with static MAC configured in the EVPN instance, the remote EVPN instance can see the MAC route information. However, after deactivating and activating the static MAC in the EVPN

instance, and then checking the MAC route information in the remote EVPN instance, no such MAC route is found in the EVPN route table. [PR1193754](#)

- On MX Series routers with EVPN, the routing protocol process might crash when MAC moves between multihomed PE routers, resulting in traffic loss. [PR1216144](#)
- An incorrect PE router is attached to an end system identifier (ESI) when the router receives two copies of the same AD/ESI route (for example, one through eBGP and another one received from an iBGP neighbor). This issue causes a partial traffic black hole and stale MAC entries. You can confirm the issue by checking the members of the ESI: `user@router> show evpn instance extensive ...` **Number of ethernet segments: 5 ESI: 00:13:78:00:00:00:00:00:01 Status: Resolved Number of remote PEs connected: 3 Remote PE MAC label Aliasing label Mode 87.233.39.102 0 0 all-active 87.233.39.1 200 0 all-active <<<< this PE is not part of the ESI 87.233.39.101 200 0 all-active.** [PR1231402](#)
- If a host is multihomed to a set of PE routers for redundancy, when the host's MAC or IP address is learned by one of these PE routers, all the PE routers that belong to this redundant set install the /32 host route pointing to its local IRB interface in the tenant's IP routing instance table as long as its local multihoming ES interface connecting to this host is up. This is the optimized behavior that can be achieved with the statement **routing-option forwarding-table chained-composite-next-hop ingress evpn** on a QFX5110 platform unless this statement is a part of Junos OS default configuration. Otherwise, without enabling this configuration statement, if a PE router is attached, the multihomed ES learns this host's MAC or IP address from the control plane through EVPN and the PE router installs the /32 host route pointing to the remote PE router where it learns the host's MAC or IP address. For a PE router attached to the multihomed ES and learned this host's MAC or IP address locally through the data plane, the PE router always installs the /32 host route pointed to its local IRB interface. [PR1321187](#)
- The issue is applicable to mac-in-mac private network-to-network (PNN) EVPN and does not affect any other scenario. When a provider backbone bridging (PBB) EVPN configuration is reloaded on MX Series routers, error logs are seen while deleting interfaces related to a backbone bridge component. These errors do not result in any functional issues. [PR1323275](#)
- PBB EVPN cannot flood traffic towards a core layer. Traffic recovers by performing **restart l2-learning**. In addition to this, there is a limitation in PBB EVPN active/active (A/A) unicast traffic forwarding. If entropy in the traffic is not sufficient, then uneven load balancing causes a problem on MH peer A/A routers. This causes a drop for return traffic. These issues are applicable to mac-in-mac private network-to-network (PNN)-EVPN and does not affect any other scenario. [PR1323503](#)
- When EVPN PE (RR) is configured as single home without ESI, EVPN BGP routes from the routing table "bgp.evpn.0" might leak into default EVPN routing table (__default_evpn__.evpn.0) causing label leak. Leak might lead to all label exhaustion and result in rpd generating a core file. [PR1333944](#)
- When you filter an EVPN route using the **show route evpn-ethernet-tag-id** CLI command, it looks for routes in all routing tables including inet.0. The EVPN route will not be present in inet.0 and the non-EVPN route will not have the Ethernet tag, which might result in an rpd process crash. [PR1337506](#)
- Bi-direction L2 traffic floods for around 5 seconds for streams from SH to MH, when **clear mac table** command is executed on MX Series router because MAC takes time to develop in the system. **clear mac table** is a disruptive command which deletes all dynamic MACs in the system. [PR1360348](#)

- On a Junos OS platform running EVPN VXLAN and Junos OS Release 17.3 software, BD override RT (specified under **protocols evpn vni-options vni <>** on QFX and **set routing-instances <> protocols evpn vni-options vni <>** on MX Series routers) will be used for export alone. To use the same RT for import, configure the same under a vrf-import policy and attach it to the routing instance. [PR1369043](#)
- Junos OS allows for auto derivation of per-VNI route targets for EVPN-VXLAN instances using the configuration **set routing-instances <NAME> vrf-target auto**. This configuration automatically creates a route target per VNI using a combination of the VNI and the device AS number. When an EBGp overlay is used, devices participating in the same EVPN is configured with different AS numbers, preventing the automatically derived route targets from matching for common VNIs. QFX Series devices allow an additional configuration ... **vrf-target auto import-as <ASN> vni-list [<VNI> | <VNI-RANGE> | all]** to specify the AS number to use for each VNI when generating the route target to overcome the different AS numbers on each devices. Currently this configuration is not supported on MX Series routers. [PR1369575](#)
- Gratuitous ARP request did not update ARP table when ARP proxy is enabled. [PR1371352](#)

Forwarding and Sampling

- When a policing filter is applied to an active LSP carrying traffic, the LSP resignals and drops traffic for approximately 2 seconds. It can take up to 30 seconds for the LSP to come up under the following conditions: (1) Creation of the policing filter and of the policing filter application to the LSP through the configuration occurs in the same commit sequence. (2) Load override of a configuration file that has a policing filter and a policing filter application to the LSP is followed by a commit. [PR1160669](#)
- When the statement **system archival configuration transfer-on-commit** is configured and the archival site is not reachable, the configuration files might be kept in the transient directory **/var/transfer/config** for retrying archival for 30 minutes. However, when the commit is more frequent within 30 minute, the commit rate is more than the file removal rate which leads to piling-up of files in **/var/transfer/config** directory. [PR1257229](#)
- In some stress test conditions, the sampled process crashes and generates a core file when connecting to Layer 2 Bitstream Access and EVPN subscribers aggressively. [PR1293237](#)
- Firewall filter is not applied as input filter to extended port when used for L2VPN. [PR1311013](#)
- This issue affects unified ISSU only when filter lists are being used. Starting in Junos OS Release 15.1F5, 15.1F6, 16.1R1 or later to Junos OS Release 17.1R2, 17.1R3, 17.2R2, 17.2X75-D50, 17.3R1 or later an error might occur that prevents firewall configuration changes from being properly applied. To avoid this issue, the configuration must explicitly set the **filter-list-template** or **no-filter-list-template** flag before the unified ISSU is done. [PR1345711](#)
- IPv6 neighbor points to a virtual tunnel endpoint (VTEP) interface even though the direct local interface to reach an IPv6 neighbor is up when a link part of the end system identifier (ESI) is flapped. [PR1350250](#)

General Routing

- When hybrid timing mode is configured (Point to Point over Ethernet plus Synchronous Ethernet), MX Series routers do not interoperate with ACX Series in native VLAN mode. [PR1076666](#)
- On chassis-based line cards, the **FI: Protect: Parity error for CP freepool SRAM** SRAM parity error might be seen. It is harmless and can be ignored. [PR1079726](#)
- The Routing Engine CPU uses chassis temperature to decide fan speed instead of Routing Engine CPU temperature. This PR has been fixed to use the real Routing Engine CPU temperature to decide the temperature threshold. [PR1230109](#)
- The following error messages occur during GRES and unified ISSU: **syslog errors @ agentd_rts_async_rtbm_msg : FLM : Failed to create private.** [PR1232636](#)
- When the virtual switch type is changed from IRB type to regular bridge, interfaces under the OpenFlow protocol are removed. The OpenFlow process (daemon) fails to program any flows. [PR1234141](#)
- After configuring PCEP following log seen **pccd: [89798] Could not decode message from rpd.** This might impact in growth of memory of pccd process over time, which can be cleared by restarting the process. [PR1235692](#)
- Sometimes, when PPPoE subscribers log-in and log-out from Junos OS Release 16.1 and later, the following messages are generated: **user@host> show log messages | match authd authd[5208]: sdb_app_access_line_entry_read_by_uifl: uifl key 'demux0.xxxxxxxx': snapshot failed (-7) authd[5208]: sdb_app_access_line_entry_read: uifl key 'demux0.xxxxxxxx': read failed.** These messages indicate that the authd process for subscriber authentication is attempting to read private data for an underlying interface that no longer exists (-7 = SDB_DATA_NOT_FOUND). These messages have no impact and can be safely ignored, where the authd process is asking the software database for a record that no longer exists. [PR1236211](#)
- On MX Series routers with the XM chipset (for example, MPC3E, MPC4E, MPC5E, MPC6E, MPC2E-NG, and MPC3E-NG), the MPC might reboot when the unified ISSU completes. [PR1256145](#)
- The following cosmetic error is observed as the output: **mshpmand[190]: msvcs_session_send: Plugin id 3 not present in the svc chain for session.** [PR1258970](#)
- The guest network function (GNF) might restart MPC9 line cards during a Routing Engine switchover in a node virtualization setup at high scale with nonstop active routing (NSR) configured in rare scenarios. [PR1259910](#)
- The issue occurs when an interface comes online and both the OAM protocol and the MKA protocol try to establish their respective sessions. Because of contention between these two protocols, OAM takes down the interface and MKA fails to establish connection (because the interface is down, it cannot send out MKA packets). [PR1265352](#)
- On an MX Series Virtual Chassis system in a scaled subscriber management scenario, if a unified ISSU is performed while BGP sessions are active and such BGP sessions are clients of the Bidirectional

Forwarding Detection (BFD) protocol, then these BGP sessions might go down and come back up again, causing traffic loss. [PR1265407](#)

- The issue occurs when the Packet Forwarding Engine is oversubscribed with an unknown unicast flood with no MAC learning, which is not a common configuration. During unified ISSU, only the Packet Forwarding Engine gets wedged. However, this issue is not seen when the Packet Forwarding Engine is oversubscribed with L3 traffic or with L2 traffic with MAC learning. [PR1265898](#)
- Currently, the broadband edge (BBE) advanced services is not supported on the node virtualization platform. Hence, mobility is disabled on the node virtualization platform base system (BSYS) and guest network function (GNF) Routing Engines. For legacy purposes, BBE functionality needs to work properly on the node virtualization platform. Reboot is required when the BSYS Routing Engine is changed to standalone Routing Engine mode (normal) and vice versa. [PR1266615](#)
- Dynamic end-point does not support Diffie-Hellman group 19, encryption algorithm aes-256-cbc and hash sha-384 in its list of default proposals. These must be configured explicitly in the configuration. [PR1269160](#)
- Sometimes l2cpd core files are generated when LLDP neighbors are cleared. [PR1270180](#)
- In a Layer 2 Bitstream Access scaling scenario, after bringing up about 12,000 subscribers, one or more FPCs reboot. [PR1273353](#)
- Incorrect counters for output packets on child links ae0 interface when configured with the new feature **revertive**. [PR1273983](#)
- When **template-refresh-rate** and **option-refresh-rate** are configured for inline J-Flow, and both the packets and seconds interval configuration options are set, the packets interval configuration does not work. [PR1274206](#)
- Interfaces might flap on the 20x1GE SFP MIC when performing a unified ISSU from Junos OS Release 17.3R1. [PR1276816](#)
- In a scaled setup, triggering a flap of the aggregated Ethernet interfaces using the commands **set interfaces ae<x> disable** and **set interfaces ae<x> enable** might result in error messages **mqchip_disable_ostream() MQCHIP(2) timed out waiting for phy_stream 1025 queue empty** on the AgentSmith platform. [PR1279607](#)
- A vmhost snapshot is taken on an alternate disk. There is no further vmhost software image upgrade. The expectation is that on the current vmhost image getting corrupted, the system boots with an alternate disk. This allows the user to recover the primary disk to restore the state. However, if the corruption is with the host root file system, the node boots with the previous vmhost software instead of booting from the alternate disk. [PR1281554](#)
- On an MX Series Virtual Chassis, while using a channelized configuration on MPC7, MPC8, and MPC9 MRATE PIC QSFP interfaces for VCP connections between members, a VCP interface needs to be configured on channel 0 of each QSFP to activate the port. [PR1283283](#)
- Due to vendor code limitation, ungraceful removing of summit MACsec TIC from a chassis might cause a crash or an unpredictable result. [PR1284040](#)

- This is in an internal change as syslog usage is deprecated. Applications have migrated to tracing for engineering debug messages or ERRMSG for customer useful or relevant messages. [PR1284625](#)
- The Routing Engine gets stuck and boots from the other solid-state drive (SSD) after a vmhost reboot. [PR1295219](#)
- When an optical carrier (OC) package upgrade is triggered when telemetry is going on, xmlproxyd might crash. It recovers automatically and xmlproxyd-related streaming restarts as the process comes up again. We recommend that you stop the streaming and then do the OC package upgrade. [PR1295831](#)
- In some MX Series deployments running Junos OS, random syslog messages are observed for FPC cards. For example, you might see **fpcx ppe_img_ucose_redistribute Failed to evict needed instr to GUMEM - xxx left**. These messages are not an issue and might not have a service impact. These messages are addressed as INFO level messages. On a Junos OS Packet Forwarding Engine, there are dedicated UMEM and shared GUMEM memory blocks. This informational message indicates some evicting events between UMEM and GUMEM and can be safely ignored. [PR1298161](#)
- Precision Time Protocol (PTP) slave is taking more than 1 hour to lock to master in a T-BC scenario. [PR1298792](#)
- User configured packet hashing options for inet family under enhanced-hash-key might not take effect for FPCs in MX Series platforms. FPC might keep using default behavior for hash calculation for IPv4 packets. [PR1302637](#)
- This type of crash indicates a simultaneous operation on an ephemeral instance. When a process wants to open an ephemeral configuration in merge view, some other activity (like purging, deletion , or recreation) is being carried out on this ephemeral instance. The occurrence of this core file is rare. [PR1305424](#)
- The message **LIBJNX_REPLICATE_RCP_ERROR** is repeated multiple times in "SYSLOG" log files in the master Routing Engine, when the backup is not reachable. Though the message is marked as ERROR in the SYSLOG, The user need not take any action on this ERROR and this will not have any impact on the SYSTEM and can ignore it. [PR1305660](#)
- Sensors belonging to the same producer (for example, BGP and MPLS coming from rpd) with the same reporting interval are not streamed in parallel but are streamed sequentially. An easy workaround is to use a different reporting rate for sensors that belong to the same producer. [PR1315517](#)
- An alarm is raised if mixed AC PEMs are present. The criteria to check whether mixed AC is present has changed. If the PEM is AC(HIGH), then the first bit of pem_voltage is set. If the PEM is AC(LOW), then the second bit of pem_voltage is set. If both the first and second bit are set, then MIXED AC is present. [PR1315577](#)
- If you make changes in **traffic-load-balance instance** services for one instance, it might lead to a refresh of existing instances. [PR1318184](#)
- A configuration change for Packet Forwarding Engine sensors in the middle of a reap cycle might cause the Packet Forwarding Engine to crash because of the invalid data access. This is related to the length of time it takes to reap the sensors. [PR1318677](#)

- Identical logs are generated and the severity of the logs are different between the two releases. The precise severity is observed in a later release. The reason to find a dissimilar severity in the earlier release is not identified. [PR1318884](#)
- The routing protocol process (rpd) might crash if OpenConfig collector for BGP telemetry is running while BGP neighbor is being deleted because of a configuration change. [PR1320900](#)
- The CLI command **request vmhost halt routing-engine other** does not achieve the intended action. [PR1323546](#)
- The following logs repeat every 5 seconds in a chassisd log. **fm_feacap_sys_feature_get:Attribute DB init not yet done, reading from pvid (id: 18) fm_feacap_sys_feature_get: Attribute key fabric.planes_per_board does not exists** [PR1328868](#)
- On a secure association key (SAK) rollover the SAK identifier displayed for the new key differs from the old key only in the last few bytes. There is no functional impact and there is no workaround. [PR1332031](#)
- In an **asymmetric cipher-suite** configuration with aes256 and aes256-xpn on MACsec peer nodes, a MACsec Key Agreement (MKA) session comes up. [PR1332156](#)
- FPC restarts and Virtual Chassis splits. The design of the MX Series Virtual Chassis infrastructure relies on the integrity of TCP connections. The reaction of the MX Series to failure situations might not be handled gracefully. If the tcp connection timeout because of jlock hog crossing boundary value (5 seconds) causing bad consequences in MX Series Virtual Chassis, then currently there are no other easy solutions to reduce this jlock hog besides enabling marker infrastructure in MX Series Virtual Chassis setup. Unfortunately, there is no immediate plan to enable a marker. [PR1332765](#)
- With certificate hierarchy, where intermediate CA profiles are not present on the device, in some corner cases, the pkid might become busy and stop responding. [PR1336733](#)
- On a next generation Routing Engine, after upgrading Junos vmhost, the AI-script gets uninstalled. You need to re-install these scripts. This is not the case on K2-RE. [PR1337028](#)
- Circuits using QSFP28-100GBASE-LR4 might find that a link does not recover after going down. Light levels fluctuate across lanes and PCS errors increase. Additionally, "Rx loss of signal alarm" will be active despite acceptable Rx levels. [PR1337327](#)
- Whenever the offline button in the Control Board is pressed for 4+ seconds, the CLI shows that the Control Board is online. There is no impact to the system other than displaying the Control Board. > **show chassis environment cb Feb 09 12:43:43 CB 0 status: State Online Master CB 0 Exhaust Temp Sensor 41 degrees C / 105 degrees F CB 0 Inlet Temp Sensor 35 degrees C / 95 degrees F CB 0 CPU DIE Temp Sensor 46 degrees C / 114 degrees F Power VDD1V5_PCH 1489 mV VDDIO 940 mV VDD3V3_PCH 3332 mV VDD2V5_AB 2489 mV VDD1V8_CLC 1803 mV VDD3V3 3292 mV VDD2V5_CD 2489 mV VDD1V2_CBC_GTX 1195 mV VDD1V8_GLS_GTX 1803 mV VDD1V2_CBC 1195 mV VDD1V8_GLS 1783 mV BIAS3V3_BP 4018 mV VDD1V2_GH 1199 mV VDD3V3_CBC 3300 mV VDD1V2_CD 1200 mV BIAS3V3 3340 mV VDD1V2_AB 1199 mV VDD5V0 5000 mV VDD1V05 1050 mV VDD1V05 1050 mV VCORE 1770 mV 12V 12285 mV 4806 mA 58923 mW CB 1 status: State Online Standby CB 1 Exhaust Temp Sensor 34 degrees C / 93 degrees F CB 1 Inlet Temp Sensor**

32 degrees C / 89 degrees F CB 1 CPU DIE Temp Sensor 46 degrees C / 114 degrees F Power Disabled.
[PR1340431](#)

- The SNMP walk for the LLDP branch might fail (timeout) if lldpRemManAddrOID contains a problem value. For example: "6.15.43.6.1.4.1.143.91.5.25.41.1.2.1.1.1" > show snmp mib walk lldpRemManAddrEntry > ... > lldpRemManAddrOID.529150.512.5.1.4.10.255.10.3 = 6.15.43.6.1.4.1.143.91.5.25.41.1.2.1.1.1. [PR1342741](#)
- On MX Series routers with a 100M SFP transceiver used on MIC-3D-20GE-SFP-E and MIC-3D-20GE-SFP-EH, the SFP transceiver might not work if it is third party. [PR1344208](#)
- When community_action is specified with community_name in netconf for an **insert after** operation, a **parse error in identifier attributes** error might be seen and the insertion fails. [PR1348082](#)
- On a next-generation Routing Engine, a failure of the hardware random number generator will leave the system in a state where not enough entropy is available to operate. [PR1349373](#)
- System might take longer time to boot or kernel might panic, if booted during broadcast storm on the management port. [PR1351977](#)
- IGMP or Multicast Listener Discovery (MLD) cannot be configured from the ephemeral database. [PR1352499](#)
- The routing protocol process (rpd) could possibly end up stuck due to repeated failures to initialize the route record module. [PR1353548](#)
- VRRP MAC filter is not seen in a Packet Forwarding Engine if aggregated Ethernet interfaces flap followed by a GRES is done; that is, before VRRP state settles down after the flap. During this time, VRRP state is backup in the master Routing Engine and VRRP state is idle in the backup Routing Engine. [PR1353583](#)
- Combination of ADF and redirect filters applied to subscribers might cause a leak in the BBE filter index. [PR1353672](#)
- vMX packet loss is seen when the active member link in an aggregated Ethernet bundle is down. [PR1354363](#)
- On MX Series routers with an MVPN environment, the rpd generates a core file when adding a p2mp-related configuration if PIM and no-forwarding VRF instances are configured. [PR1354629](#)
- If aggregated Ethernet is configured in link-protection backup-state down, the aggregated Ethernet operational state is down even when the member interfaces configured under the aggregated Ethernet are down. [PR1354686](#)
- The jsscd static-subscribers do not properly update firewall information on Packet Forwarding Engine when dynamic configuration changes are made to active subscribers. [PR1354774](#)
- The **ipv4-flow-table-size** is used to configure the size of the IPv4 flow table in units of 256,000 entries. However, in inline J-Flow scenario, if the statement **ipv6-extended-attrib** is configured, changing flow table configuration or clear the flow entries might lead to the condition that even the **ipv4-flow-table-size** has been changed to a number larger than 149, the maximum number of IPv4 flows still remains at 37372900. [PR1355095](#)

- Configuring PPTP-ALG on MX Series routers service box might cause the MS-MPC PIC to crash. [PR1356133](#)
- On an MX Series platform, if an SNMP trap is enabled, i2c messages from power entry module (PEM) or power supply module (PSM) might be seen. [PR1356259](#)
- When a demux interface is brought over a static pseudowire underlying interface, then the applicable port is changed from tagged to untagged. A deletion and re-creation of the static pseudowire underlying interface is triggered. It was noticed that subscribers could not log back in after the configuration was changed. [PR1356980](#)
- On enabling hidden configuration statement **set chassis power-off-ports-on-no-master-re**, MPC7E cards might crash during switchover with two or more iteration which is inconsistent. [PR1358451](#)
- Unified ISSU from Junos OS Releases 17.4R1, 17.3R1 and 17.3R2 to 18.2R1 for MX Series platforms might cause FPCs to go offline during unified ISSU. In order to avoid the same, 2-step unified ISSU is recommended, Junos OS Releases 17.4R1, 17.3R1 or 17.3R2 to 18.1R1 is the first step and second step is from Junos Os Release 18.1R1 to Junos Os Release 18.2R1 [PR1359282](#)
- The configurations of bridging routing instances having aggregate Ethernet IFLS(6400IFLs) and IRB instances, all from a single FPC, the CPU utilisation of the FPC stays at 100 percent for 4 minutes. The behavior from PFEMAN of FPC has the processing time spiked on IF IPCs and this seems to be the case of MPC7E from Junos OS Release 16.1R1 or prior releases. After 4 minutes, the CPU utilisation comes down and the FPC is normal. Therefore, this scale configuration on MPC7E takes settling time of more than 4 minutes. [PR1359286](#)
- FRU-model-name are not displayed for few of the FRU's. [PR1359300](#)
- CPS downgrade is observed on LAC because Routing Engine overdrives the FPCs processing capacity. [PR1360786](#)
- Back up might panic and slip to db-prompt following a fail-over. Impact is contained since the prerequisites to foul router are not easily convened, but nevertheless it can happen. Some of the known scenarios involve are back to back GRES with specific configuration, commit and rollback the configuration. [PR1362741](#)
- FRU model for midplane is not displayed. [PR1365303](#)
- There is a possibility of inter-vlan traffic drop when ESI value is changed. It is not common to change the ESI value in the running network. However, if ESI value is changed, it is known that for a while there will be a traffic disruption. In problem state, it might be a little longer (maximum arp/nd ageout) and might go unnoticed. [PR1366094](#)
- On a unified ISSU to this release, there could be some impact to forwarding of packets of some destinations. [PR1366811](#)
- The issue is seen under the following conditions: after performing a GRES, while restarting chassisd, and while rebooting the Routing Engine. Typically, the following benign error messages are observed on the backup Routing Engine when there are no Packet Forwarding Engine on the Routing Engine or when the Packet Forwarding Engine is rebooting.

- 1431:Jun 26 10:45:31 alitalia1 kernel: rts_marker_request: ADD of MARKER with seqno 770 failed
- 1432:Jun 26 10:45:31 alitalia1 kernel: rts_marker_request: ADD of MARKER with seqno 772 failed [PR1369283](#)
- When FPC is booting up (either during a unified ISSU or router reboot or FPC restart), i2c timeout errors can be noticed. These errors are seen as i2c action is not completed as device was busy. Once card is up all the i2c transactions to the device occurred without interruptions. Hence, no periodic failure is observed. There is no functional impact and these errors can be ignored. [PR1369382](#)
- In some configurations, a unified ISSU prepare time on MPC5E takes longer than usual. As a result, the chassisd triggers restart or crash of the MPC. The unified ISSU completes after the crash. [PR1369635](#)
- Creation of symlink occur during boot up of the system. However, chassisd tries to recreate it everytime the chassis restarts. As symlink is already available, corresponding system-call returns the error. The log message is cosmetic and has no functional impact. [PR1369853](#)
- Periodic monitoring of S.M.A.R.T attributes for mSATA SSD's in the PMB fails for MPC7 on MX Series routers. FPCs and NGCB fails on PTX5000. No alarm is generated if S.M.A.R.T attribute of the SSD reaches the threshold. There is no functional impact on the system because of this issue. [PR1370157](#)
- Every L2BSA subscriber creates 2 interfaces, DVLAN and RTSOCK with the same subunit (same interface name). Initially, the CLI output for **show interfaces extensive** displayed the filter information on both the DVLAN and RTSOCK interfaces. Functionally, the filter information should only be displayed on DVLAN interface. [PR1372527](#)
- The MS and AMS logical interfaces does not come up when you configure packages like url-filtering in chassis FPC hierarchy. Example: fpc 5 { pic 0 { adaptive-services { service-package { extension-provider { package jservices-urllf; } } } }. The issue is that mounting the **/var/db/*** contents to the pic fails. This is because of nfs_mount time out and therefore services logical interfaces for url-filtering will not come up. [PR1374976](#)

High Availability (HA) and Resiliency

- Virtual machine generates a core file on backup Routing Engine. Though it is not critical, it might impact NSR functionality. This can be hit in particular scenarios like back-to-back GRES with specific configuration, commit and rollback the configuration. This might not impact the production Routing Engine as there is a core file generated on backup. [PR1269383](#)
- The error **error: not enough space in /var on re1** is observed while doing a unified ISSU upgrade. As a workaround, make sure that space available in /var is twice the size of target image. This is the basic requirement for the unified ISSU to proceed. [PR1354069](#)

Infrastructure

- The configuration statement **set system ports console log-out-on-disconnect**, logs the user out from the console and closes the console connection. If the configuration statement **set system syslog console any warning** is used with the earlier configuration and when there is no active telnet connection to the console, the process tries to open the console and hangs as it waits for a "serial connect" that is received only by doing a telnet to the console. As a workaround, remove the later configuration by using **set system syslog console any warning**, which solves the issue. [PR1230657](#)
- The syslog messages are observed when one of the following CLI commands is executed: **system syslog file messages kernel any** or **system syslogfile messages any any**. These syslog messages do not indicate any functionality, breakage, or impact. If you need to enable **anyany**, then you need to skip these logs with an appropriate match condition. [PR1239651](#)
- The issue is seen when the Openconfig package is installed. When the package is installed, the analytics of configuration goes to default ephemeral db, while all the daemons read the configuration through merge view. [PR1296702](#)
- In rare incident, the MX Series routers might observed a crash after multicast traffic failover upstream AR Deactivate MPLS. [PR1351611](#)
- When validating an older Junos OS Release, the **set_flags function** might not be available. This is harmless but results in noise, where unified ISSU cannot tolerate. A stub function avoids the issue. [PR1366837](#)

Interfaces and Chassis

- Junos OS now checks logical interfaces information under the aggregated Ethernet interface and prints only if it is part of it. [PR1114110](#)
- During the configuration change and reuse of the VIP address on an interface, stop the configuration do a commit and then add the interface address configuration in the next commit. [PR1191371](#)
- In a VPLS multihoming scenario, the CFM packets are forwarded over the standby PE device link, resulting in duplicate packets or a loop between the active and standby link. [PR1253542](#)
- On using LSQ interface when sending a traffic with over subscription, out of sequence packets are seen. [PR1258258](#)
- In Junos OS Release 14.2R5 and later maintenance releases and in Junos OS Release 16.1 and later mainline releases with a connectivity fault management (CFM) configuration a cfmd crash might occur after an upgrade. This issue is because of the old version of **/var/db/cfm.db**. [PR1281073](#)
- In a subscriber management scenario with demux configured, in the case where subscribers belonging to one aggregated Ethernet interface are migrated to a new configured aggregated Ethernet interface, subscribers might fail to access the device after deleting the old aggregated Ethernet configuration. [PR1322678](#)

- The Error message **ppman_cfm_start_inline_adj: Failed to add Inline adj for CFM, pkt-len=0** is observed in some cases. But there is no functional impact. Sessions and adjacency might get programmed inline subsequently. [PR1358236](#)
- CLI allows to configure more than 2048 sub-interfaces on lag interface from Junos OS Release 17.2R1 and this is not expected. [PR1361689](#)
- When a router is rebooted or when a router is loaded with interface, service and OAM MIP configuration in a single shot with MIP on CCC interface, LTM messages are not forwarded by the PE device that generates a core file (peer PE) when originated from CE side. [PR1369085](#)
- On MX Series routers, syslog errors **vrpman_ifcm_send_message: Send to IFCM failed** are observed after rebooting MX480 router with Junos OS Release 17.3R3.7 image. [PR1373920](#)

Layer 2 Ethernet Services

- This issue occurs when running LACP between Juniper Networks and Cisco devices with different timers (Juniper Networks fast and Cisco slow) on both sides. The Cisco side it takes almost 90 seconds to bring the interface down from the bundle. When one interface is removed from the LAG on the Juniper Networks side, the lead on the Cisco side needs to time out to bring the interface down from the bundle. This results in unexpected outage behavior on the network. [PR1169358](#)
- After changing the underlying physical interface (IFD) for a static VLAN demux interface, the NAS-Port-ID formed is based on the previous physical interface. [PR1255377](#)
- The internal change as syslog usage is deprecated, there might be a customer impact because of the syslog usage in automation. Applications have migrated to tracing for engineering debug messages or ERRMSG for customer useful/relevant messages. The customer is advised to migrate to new ERRMSG definitions as appropriate. [PR1284592](#)
- Whenever an MC-aggregated Ethernet interface is deactivated or activated on an MC-LAG node, once the MC-aggregated Ethernet interfaces are back up, the system clears neighbor discovery entries on the ICL. This action triggers a neighbor discovery solicit and thereby neighbor discovery entries are learned on the MC-aggregated Ethernet interface. As a workaround, clear neighbor discovery entries on the ICL whenever MC-aggregated Ethernet interfaces have been deactivated or activated on MC-LAG nodes. [PR1294958](#)
- In a scaled subscriber management log in and log out scenario, some dhcpv6 subscribers might fail to bind. It is observed that for these dhcpv6 subscribers, the underlying IPv6 ncp subscriber negotiation has failed. [PR1357998](#)
- When adding an interface to an aggregate bundle, there is a chance forwarding through the bundle might be affected for an extended period of time, sufficient for an LDP or BGP session to go down. [PR1373564](#)

Layer 2 Features

- This issue is for router equipped with following line cards: T4000-FPC5-3D, MX-MPC3E-3D, MPC5E-40G10G, MPC5EQ-40G10G, MPC6E, and MX2K-MPC6E. If the router is working as a VPLS PE device, because of MAC aging every 5 minutes, the VPLS unicast traffic is flooded as unknown unicast every 5 minutes. [PR1148971](#)
- After an LDP signaling flap, an LDP-VPLS pseudowire might remain stuck in NP state instead of coming up because of the control word negotiation. This problem could happen if the local device is configured to prefer control word while the remote device does not support control word. When the pseudowire attempts to reestablish, control word negotiation normally selects the required mode to ensure compatibility between the local and remote devices. In unusual circumstances, the negotiation can deadlock resulting in the pseudowire remaining in NP state until the operator takes corrective action. [PR1354784](#)
- Backup router is not expected to have any MAC. But, once active router is rebooted and it is fully recovered, back router still has some MACs. [PR1356726](#)
- In scaled scenario, 16000 routing instances with 128000 FEC128 LDP hierarchical virtual private LAN service (H-VPLS) during unified ISSU traffic loss might be seen. [PR1338290](#)

MPLS

- MPLS point-to-multipoint(P2MP) LSP is composed of multiple source-to-leaf (S2L) sub-LSPs. Whenever one sub-LSP is in down state, the ingress router tries to re-signal all the sub-LSPs with a new LSP ID. While re-signaling this new P2MP LSP, if any PathErr is received from any newly signaled sub-LSP, then the ingress router tears down the whole P2MP LSP and reverts back to the older LSP. It causes the sub-LSP that remain down forever. [PR861577](#)
- When using **mpls traffic-engineering bgp-igp-both-ribs** with LDP and RSVP both enabled, CSPF for interdomain RSVP LSPs cannot find the exit area border router (ABR) when there are two or more such ABRs. This causes the interdomain RSVP LSPs to break. RSVP LSPs within the same area are not affected. As a workaround, you can either run only RSVP on OSPF ABR or IS-IS L1/L2 routers and switch RSVP off on other OSPF area 0/IS-IS L2 routers, or avoid LDP completely and use only RSVP. [PR1048560](#)
- The issue occurs when GRES is done between the master and backup Routing Engines with different memory capabilities. For example, one Routing Engine has only enough memory to run routing protocol process (rpd) in 32-bit mode while the other is capable of 64-bit mode. The situation might be caused by using Junos OS Release 13.3 or later with the configuration statement **auto-64-bit** configured, or by using Junos OS Release 15.1 or later without the configuration statement. Under these conditions, the rpd might crash on the new master Routing Engine. As a workaround, use the CLI command **set system processes routing force-32-bit**. [PR1141728](#)
- When **minimum-bandwidth** and **bandwidth** commands are present in the configuration, the bandwidth selection of the LSP is inconsistent. [PR1142443](#)

- In a CE-CE setup, traffic loss might be observed over a secondary LSP on a primary failover. [PR1240892](#)
- Because of the current way of calculating bandwidth, you see a minimal discrepancy between MPLS statistics and adjusted bandwidth reported. The algorithm is enhanced so that both values match 100 percent. [PR1259500](#)
- With nonstop active routing (NSR), when a routing protocol process (rpd) restarts on the master Routing Engine, rpd might also restart on the backup Routing Engine. [PR1282369](#)
- In case of CSPF disabled LSPs, if the primary path ERO is changed to unreachable strict hop, sometimes the primary path stays up with the old ERO. The LSP does not switch to standby secondary. [PR1284138](#)
- If there are some LSPs for which a router has link protection available and when primary link failure is caused by an FPC restart, a core file might be generated. [PR1317536](#)
- If an inet address is not configured for the gr-interface, the gr-interface borrows address from loopback interface. From Junos OS Release 16.1R1, the RSVP creates a node-neighbor by default. There are duplicate neighbors with the same IP address since the gr-interface borrows address from loopback interface. The RSVP path lookup might fail because it gets confused with the node neighbor presence. So, the RSVP LSP might not come up when it goes through the gr-interface which is the borrowing address from the loopback interface. [PR1340950](#)
- The LSP configuration cannot update its admin-group when the global admin-group (under MPLS) is changed. Hence, LSP does not come up. [PR1348208](#)
- Packets destined to the master Routing Engine might be dropped in the kernel because of excessive network traffic on the internal Ethernet interface. This excessive traffic results from a routing protocol process (rpd) requesting MPLS traffic statistics from all the online FPCs, when the jnxLdp* SNMP MIBs are queried. [PR1359956](#)

Platform and Infrastructure

- When using the **show | compare** method to commit, part of configuration might be treated as noise and return a syntax error. [PR1042512](#)
- In configurations with IRB interfaces, during times of interface deletion (for example, FPC reboot), the Packet Forwarding Engine might log errors stating **nh_ucast_change:291Referenced I2ifl not found**. This condition should be transient, with the system reconverging on the expected state. [PR1054798](#)
- When certain hardware transient failures occur on an MQ chip-based MPC, traffic might be dropped on the MPC, and syslog errors **Link sanity checks** and **Cell underflow** are reported. There is no major alarm or self-healing mechanism for this condition. [PR1265548](#)
- This issue occurs when 120 bridge domains (among a total of 1000 bridge domains) have XE or GE links toward the downstream switch and LAG bundles as uplinks toward upstream routers. The XE or GE link is part of the physical loop in the topology. Spanning tree protocols such as VSTP, RSTP, and MSTP are used for loop avoidance. Some MAC addresses are not learned on DUT when LAG bundles that are part

of such bridge domains are flapped and other events such as spanning tree root bridge changes occur. [PR1275544](#)

- With unified ISSU, a momentary traffic loss is expected. In EVPN E-Tree, in addition to traffic loss, the known unicast frames might be flooded for around 30 seconds during a unified ISSU before all forwarding states are restored. This issue does not affect BUM traffic. As a workaround, nonstop bridging (NSB) can be configured at **[set protocols layer2-control nonstop-bridging]**. This reduces traffic flood to around 10 seconds in a moderate setup. [PR1275621](#)
- Due to a transient hardware error condition the **CPQ Sram parity error** and **CPQ RLDRAM double bit ECC error** syslog errors on the MQ chip raise a major CM alarm. [PR1276132](#)
- The prefix apply-path is not inherited under a policy after a commit. [PR1286987](#)
- Every load override increases the reference count by 1. After it reaches the maximum value (65,535), the mgd crashes and the session is killed. There is no impact for a new session. [PR1313158](#)
- This system limitation is due to high system load and aggressive IS-IS hello timer. As a workaround, increase the hello timer so the adjacent interface does not flap. [PR1314650](#)
- On an EVPN VXLAN enabled MX Series router, if the underlying interface for the VXLAN tunnel is a LACP enabled aggregated Ethernet interface with multiple members, and one of the member is flapped. There might be momentary IPv4 or IPv6 inter-vni traffic loss. [PR1326572](#)
- Traffic statistics might not match on PS after clearing interface statistics. [PR1328252](#)
- In EVPN E-tree, traffic loss is seen on deactivating a CE-facing interface both with NSR enabled and in a normal scenario. CE interface, which is a leaf interface, is deleted completely and added back to restore the same old state logical interface being part of the same EVPN. The leaf-to-leaf traffic might not get blocked. [PR1330134](#)
- While downgrading a Junos OS platform from a later release to Junos OS Release 17.3R2, the box goes into amnesiac state. This issue is not seen when upgrading from Junos OS Release 17.3R2. [PR1341650](#)
- MPC5-inline-ka PPP echo requests are not transmitted when anchor point is lt-x/2/x or lt-x/3/x in a pseudowire deployment. [PR1345727](#)
- MGD memory usage shown as increased by about 450 MB when run DT CST test over weekend (>72 hours). [PR1352504](#)
- It is expected to see a few transient FI Cell underflow errors during a unified ISSU as long as they do not persist. [PR1353904](#)
- In a Layer 3 VPN topology, traceroute to a remote PE device for a CE-facing network see the ICMP TTL expired reply with a source address of only one of the many CE-facing networks. In Junos OS Release 15.1R5, 16.1R3, 16.2R1 and later, there is a kernel sysctl value, icmp.traceroute_l3vpn. Setting this to 1 will change the behavior to selected an address based on destination specified in the traceroute command. [PR1358376](#)
- On MX Series routers running Junos OS Release 17.3R3, moving from baseline configuration to EVPN scaled (4000 VLANs) configuration with multihoming, the newly elected designated forwarder might

take up to 90 seconds to resume forwarding BUM traffic. The time required for convergence is proportional to the scale used, so a lower scale incurs a smaller dark window. Workaround for faster convergence with high scale, distributing the configuration across several FPCs can potentially bring down the BUM traffic drop from 90 seconds to a significantly lower value. [PR1362934](#)

- Qmon Sensors are not working when hyper-mode is enabled. [PR1365990](#)

Routing Protocols

- When you configure damping globally and use the import policy to prevent damping for specific routes, and a peer sends a new route that has the local interface address as the next hop, the route is added to the routing table with default damping parameters, even though the import policy has a non-default setting. As a result, damping settings do not change appropriately when the route attributes change. [PR51975](#)
- Continuous soft core files might be generated due to a bgp-path-selection code. The routing protocol process (rpd) forks a child and the child asserts to produce a core file. The problem is with route ordering and it is auto-corrected after collecting the soft-assert-core file, without any impact to the traffic or service. [PR815146](#)
- On MX Series routers, when an instance type is changed from VPLS to EVPN, and in the same commit an interface is added to the EVPN instance, the newly added EVPN interface might not be able to come up. [PR1016797](#)
- The rpd might crash when running rpd for a long time (such as two years without a restart). [PR1092009](#)
- With Shared Risk Link Group (SRLG) enabled under corner conditions, after executing the command **clear isis database**, the rpd might crash because the IS-IS database tree gets corrupted. [PR1152940](#)
- The VRF-related routes, which are leaked to the global inet.0 table and advertised by the access routers are not being advertised to global inet.0 table on the core layer. [PR1200883](#)
- JTASK_SCHED_SLIP for rpd might be seen on restarting routing or disabling OSPF protocol with scaled BGP routes in an MX104 router. [PR1203979](#)
- In Junos OS Release 16.1R5 and later, the routing protocol process (rpd) generates core files in the ASBR when BGP is deactivated in the ASBR before all stale labels have been cleaned up. Junos OS Release 16.1R6, 16.1R5_S(X+1 SR if any and later, the issue will be analyzed, fixed, and soaked for these releases. [PR1233893](#)
- 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 and OSPF are in sync state because it is observed that "IGP interface down" with ldp-synchronization is 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, "IGP interface down" is the reason because although LDP notified OSPF that LDP synchronization was achieved, OSPF was not able to take note of the LDP synchronization notification. This occurred because the OSPF neighbor was not up yet. The issue is under investigation. [PR1256434](#)

- When switchover and zeroize are done in quick succession, "zeroize" deletes the databases. If dfwd is going to start SIHUP processing after the zeroize, it generates a core file as a database is not present. Zeroize should be done when the system is in stable state; that is, signups processing by daemons is completed. [PR1262385](#)
- Performance degradation occurs during computation of LFA and RLFA. This issue does not impact functionality. [PR1264564](#)
- When generating SNMP traps or notifications for BGP events from the jnxBgpM2 MIB, Junos OS was not properly emitting OBJECTS of type InetAddress with the expected length field. This causes compliant SNMP tools to be able to parse the contents of those OBJECTS properly. In particular, the length field for the InetAddress OBJECT-TYPE was omitted. Using the **set protocols bgp snmp-options emit-inet-address-length-in-oid** command causes these OBJECTS to be emitted in a compliant fashion. Given the length of time that this error has been in place, it was decided to leave the existing non-compliant behavior in place to avoid breaking tools that had accommodated the existing behavior as the default. [PR1265504](#)
- BGP monitoring output no longer sends withdrawals when station peer monitoring is disabled. The BMP session would send both peer down events as well as route withdrawals when a peer monitoring was disabled through a configuration event. After that commit, only the peer down events are sent. [PR1265783](#)
- When **route-distinguisher-id** is configured and a VRF with a route distinguisher is automatically assigned with the **auto-rdfeature** configured, the MX Series BNG allows commit followed by rpd process crash. [PR1278582](#)
- Two multicast tunnel (mt) interfaces are seen for each of the PIM neighbors after VPN-Tunnel-Source activation or deactivation. However, ideally, the same tunnel source should be used for both IPv4 and IPv6 address families if both are using the same PIM tunnel. [PR1281481](#)
- This is in an internal change as syslog usage is deprecated, however, there might be customer impact because of syslog usage in automation. Applications have migrated to tracing for engineering debug messages or ERRMSG for customer useful or relevant messages. The customer is advised to migrate to new ERRMSG definitions as appropriate. [PR1284621](#)
- When eBGP multihop sessions exchanging EVPN routes are configured, a core file might be generated as a result because of an internal error. [PR1304639](#)
- An MX104 is connected to an SRX1500. IS-IS is running between these devices and BFD has been configured between the IS-IS peers. Unfortunately, BFD is not coming up between these devices successfully. [PR1312298](#)

- In Resource Public Key Infrastructure (RPKI) scenario, the validation replication database might have much more entries than the validation database after restarting RPKI cache server and the validation session is reestablished. [PR1325037](#)
- When route target filtering (RTF) is configured for Virtual Private Network (VPN) routes and multiple BGP sessions flap, there is a slight chance that some of the peers might not receive the VPN routes after the flapped sessions come up. [PR1325481](#)
- When a **clear validation database** was issued back to back multiple times, it ends up with partial validation database (some validation entries were missing). This eventually is recovered after up to 30 minutes (half of the record lifetime) when we did periodical full updates. [PR1326256](#)
- When configuring anycast and prefix segments in SPRING for IS-IS, prefix-segment index 0 is not supported, even though the user is allowed to configure 0 as an index. [PR1340091](#)
- Different AIGP values are observed on executing the CLI commands **show route receive-protocol bgp** and **show route detail** outputs. [PR1342139](#)
- During a unified ISSU at MX Series Virtual Chassis, the MX-VC side might clear the TCP connection causing BGP peerings to flap. [PR1368805](#)

Services Applications

- Session counters for cleartext traffic are not updated after decryption. Decrypted packet count can, however, be obtained by running the following command **show security group-vpn member ipsec statistics**. [PR1068094](#)
- We do not recommend configuring **ms- interface** when the AMS bundle in one-to-one mode has the same member interface. [PR1209660](#)

Subscriber Access Management

- In a PPPoE subscriber scenario with a large number of subscribers (for example, 3000), during operation of log in and log out, some subscribers might be stuck in an error state of **Terminated**. This issue impacts the traffic for these error subscribers. [PR1262219](#)
- Multiple RADIUS servers having different dynamic request port is not supported. However, due to missing configuration constrain checks, customers might end up in a configuration where different dynamic request ports are configured for different RADIUS servers. Currently Junos OS reads **dynamic-request-port** configuration for the first RADIUS server and ignores the rest. In the event no **dynamic-request-port** is configured, it defaults to port 3799. [PR1330802](#)

User Interface and Configuration

- CLI session might die while issuing command **show configuration | compare rollback 1**. This happens when **persist-groups-inheritance** is enabled in the system. [PR1331716](#)

VPNs

- In a multicast VPN based with BGP (next-generation MVPN) scenario with only an SPT mode configuration, under certain conditions the PIM register-stop packet might be sent before the Source Tree Join (Type-7) packet, which might cause some multicast packets to drop. [PR1238916](#)
- Based on code analysis, in a scale scenario it is possible that a protocol on a master Routing Engine might have allocated as released a label. The backup Routing Engine might have allocated the label but is still in process of the removal of the label. Prior to this, if the master Routing Engine allocates the same label to some other protocol synchronizes to the backup, it might not be able to allocate the label. In such scenario, MVPN does not handle a label allocation failure on the backup, which leads to the current problem. This is not easily reproduced and hence cannot be confirmed. A possible workaround is to give sufficient time for the backup to properly remove all labels after deactivate instance and then reactivate instance. It is possible it can happen on rpd restart on the master, in which case rpd backup should also be restarted. In the event it has happened, the back up would restart and come backup and be synchronized with the master. Forwarding on the master would not be affected. [PR1258882](#)
- The L2 circuit or the CE facing interface might flap repeatedly and cause the packets to drop if the configuration **asynchronous-notification** is configured on the PE device. [PR1282875](#)
- When switching from Layer 2 circuit to EVPNs VPWS, deactivate and activate the instance. [PR1312043](#)
- With NSR enabled and a Layer 2 circuit configured, an rpd crash might be observed on the backup Routing Engine when you change the Layer 2 circuit **virtual-circuit-id** and then commit the changes. [PR1345949](#)
- Core file generated is seen on backup Routing Engine on label allocation, restarting routing on master when NSR is enabled. [PR1351425](#)

SEE ALSO

[New and Changed Features | 103](#)

[Changes in Behavior and Syntax | 135](#)

[Known Behavior | 145](#)

[Resolved Issues | 174](#)

[Documentation Updates | 214](#)

[Migration, Upgrade, and Downgrade Instructions | 215](#)

Resolved Issues

IN THIS SECTION

- Resolved Issues: 17.3R3 | [174](#)
- Resolved Issues: 17.3R2 | [196](#)
- Resolved Issues: 17.3R1 | [209](#)

This section lists the issues fixed in the Junos OS main release and the maintenance releases.

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

Resolved Issues: 17.3R3

Application Layer Gateways (ALGs)

- IKEv2 negotiation might fail with IKE ESP ALG enabled in IKEv2 redirection scenario. [PR1329611](#)

Class of Service (CoS)

- CoS wildcard configuration is applied incorrectly after router restart. [PR1325708](#)
- Remove CoS IDL from the jet IDL package and update the documentation for the same. [PR1347175](#)
- The Routing Engine might get into amnesiac mode after restarting if **excess-bandwidth-share** is configured. [PR1348698](#)
- CoS traffic control profiles fail to apply on an aggregated Ethernet interface in a specific condition. [PR1355498](#)

EVPN

- EVPN traffic mapping to specific LSPs does not work. [PR1281415](#)
- Local preference for EVPN type-5 route might cause unexpected results if BGP multipaths are configured. [PR1292234](#)
- BGP route refresh request might not be sent after modifying the route-target. [PR1300332](#)
- The traffic might be dropped after receiving an updated ARP route update packet from peer Layer 3 gateway in EVPN and VxLAN scenario. [PR1306024](#)

- The rpd might crash after restarting the rpd process in EVPN environment. [PR1320408](#)
- Discard EVPN route is installed on local PE device after connection flaps on a remote PE in a multihome EVPN topology. [PR1321125](#)
- If host is multihomed then all PE devices should install the /32 host IP address pointing to its local IRB interface as long as its local multihomed ES interface is up. [PR1321187](#)
- FPC might crash while deleting VPLS configuration. [PR1324830](#)
- Core link flap might result in an inconsistent global MAC count. [PR1328956](#)
- On deactivated ESI for PS at physical interface level, encountered routing protocol process generates a core file for EVPN VPWS PWHT. [PR1332652](#)
- On doing a **restart routing**, the routing protocol process (rpd) generates a core file in provider edge (PE) router that has EVPN-VXLAN configuration. [PR1333331](#)
- The rpd process might crash on the new master in an EVPN-VXLAN deployment after performing a GRES. [PR1333754](#)
- The routing protocol process (rpd) crash and generates a core file on backup Routing Engine while any configuration changes on master Routing Engine. [PR1336881](#)
- In EVPN and VXLAN environment, BFD flap cause VTEP flap and crashes Packet Forwarding Engine. [PR1339084](#)
- Traffic loss might be observed in EVPN VPWS scenario if the remote PE devices interface comes down. [PR1339217](#)
- The traffic might get dropped as the core is down [PR1343515](#)
- The rpd might crash if the IRB interface and routing instance are deleted together when committed. [PR1345519](#)
- Traffic might be lost on layer2 and layer3 spine node in multi-home EVPN scenario. [PR1355165](#)

Forwarding and Sampling

- The mib2d process might crash during SNMP walk on committing or rollbacking. [PR1286448](#)
- Observing pfd core file in `pfed_process_session_state_notification_msg`, `pfed_timer_manager_c::remove_serv_id`, `pfed_delete_timer_id_by_serv_sid` (`serv_sid=0`, `serv_info=0x0`) at `../../../../src/junos/usr.sbin/pfed/pfed_timer.cc:16`. [PR1296969](#)
- Remote CE1 MAC address might take long time to clear post MAC. [PR1304866](#)
- Dfwd might crash during execution of **show firewall templates-in-use** command. [PR1305284](#)
- The second archive site in the accounting-file configuration is not used when the first one uses SFTP and is not reachable. [PR1311749](#)
- The FPC CPU might reach 100 percent constantly if shared bandwidth policer is configured. [PR1320349](#)
- The error messages about `dfw_gencfg_handler` might be seen during unified ISSU. [PR1323795](#)

- EVPN VXLAN IPv6 neighbor points to vtep interface even though the direct local interface to reach IPv6 neighbor is up. [PR1350250](#)
- Some firewall filter counters might not be created in SNMP. [PR1335828](#)
- The error logical interfaces under VPLS might be blocked after MAC moving if the logical interfaces are on the same physical interface. [PR1335880](#)
- The commands **clear ethernet table**, **clear bridge table**, **clear evpn table in evpn**, and **vxlan instance** has issues. [PR1341328](#)
- Commit failed when attempting to delete any demux0 unit numbers which are greater or equal to 1000000000. [PR1348587](#)
- The remote MAC might not be added in forwarding table which causes traffic drop in EVPN scenario with RSVP and CBF configured. [PR1353555](#)
- Packet Forwarding Engine process (pfed) creates dummy interface accounting records on the backup Routing Engine. [PR1361403](#)

General Routing

- Memory leak on L3vpn configuration commit for L3VPN scaling test. [PR1115686](#)
- No warning is raised when the bridge family is configured with interface-mode trunk but without vlan-tagging or flexible-vlan-tagging. [PR1154024](#)
- Unexpected MobileNext Gateway Activation license alarm when TDF gateway is configured. [PR1162518](#)
- SNMP trap sent for "PEM Input failure" alarm is not generated when single input feed fails on MX960. [PR1189641](#)
- The replacement PIC might bounce when PIC PB-4OC3-4OC12-SON-SFP (4x OC-12-3 SFP) is replaced with PB-4OC3-1OC12-SON2-SFP (4x OC-3 1x OC-12 SFP) and committed. [PR1190569](#)
- The agentd process crashes generating a core file. [PR1197608](#)
- Unable to deregister sub error (131072) for error (0x1b0001) for module MIC. error messages seen on MPC5E card. [PR1221337](#)
- In Junos OS multiple vulnerabilities in stunel is observed. [PR1226804](#)
- The error log **cc_mic_irq_status: CC_MIC(5/2) irq_status(0x1d) does not match irq_mask(0x20), enable(0x20), latch(0x1d)** is seen continuously for "MIC-3D-4OC3OC12-1OC48". [PR1231084](#)
- False AC PEM failure(status bits: 0xff) alarm/SNMP trap seen with MX5, MX10, MX40, and MX80 router platforms. [PR1231893](#)
- Tracking PR for enabling mobiled for MX Series Virtual Chassis environment. [PR1241857](#)
- chassisd[9132]: LIBJSNMP_NS_LOG_NOTICE: NOTICE: netsnmp_ipc_client_connection: unix connection error: socket(-1) main_session(0x9812f80) error messages are seen after chassis-control restart. [PR1243364](#)

- vMX FPC core file might be generated - **panic(format_string=format_string@entry=0x9e509c4 "Thread %s attempted to %s with irq priority at %d\n")**. [PR1263117](#)
- The load-based throttling feature is not enabled by default. [PR1271739](#)
- Error messages are observed on vty session while running script for IGMP snooping over EVPN-VXLAN. [PR1276947](#)
- The rpd KRT asynchronous queue might stall, impacting synchronization between RIB and FIB. [PR1277079](#)
- The syslog messages **jnh_vbf_flow_get_oif_index: Rollback cmd not found for flow** are generated by MPC during subscriber login. [PR1278580](#)
- BSYS logs GNF owned pics do not support power off configuration at commit when no such configuration is present. [PR1281604](#)
- The kernel might crash in a rare corner case. [PR1282573](#)
- The enhancement of reporting total SBE errors when the corrected singlebit errors threshold of 32 is exceeded for MPC7E, MPC8E, and MPC9E. [PR1285315](#)
- The oneset and leaf-list configuration might not get deleted with delete operation through JSON. [PR1287342](#)
- In an EVPN or VXLAN, inter-vrf traffic blackhole occurs after routing is restarted repeatedly on redundant gateways. [PR1289091](#)
- The routing protocol process (rpd) might generate a core file while restarting the process. [PR1291110](#)
- Restart chassisd results in FPC restarting multiple times with GRES enabled. [PR1293314](#)
- During PPPoE subscriber login errors like [**vbf_flow_src_lookup_enabled**] and [**failed to find iff structure, ifl**] were seen on FPC. [PR1294710](#)
- TACACS remote user is unable to run JET applications because of a bad stored heap. [PR1296237](#)
- Shmlog does not work on MX5, MX10, MX40 except MX80 product model. [PR1297818](#)
- Some random number of ports on MPC7E-10G card might not come up after the remote system and line card restarts or interface flap. [PR1298115](#)
- The log message about shutdown time is incorrect when system exceeds chassis over temperature limit. [PR1298414](#)
- The error messages about PEM might be seen in MX Serie splatform with AC PEM. [PR1299284](#)
- The rpd might crash when NSR is enabled and routing instance specific configurations are committed. [PR1301986](#)
- The log message **jam_cache_get.636 ERR:entity 0x997 not found, get cache failed** is continuously seen in jam_chassisd log-file. [PR1302975](#)
- The multicast resolve-rate value might go back to default after system upgrade or reboot. [PR1303134](#)
- The kernel log GENCFG messages with severity 1 (alert) might be seen. [PR1303637](#)

- The fabric planes might go into "check" state after restarting the line cards with SFB2 used on MX2010 and MX2020 platform. [PR1304095](#)
- The CLI **start shell pfe network fpc** command do not work on MX960. [PR1306236](#)
- FPC syslog errors with **pfeman_inline_ka_steering_gencfg_handler: nh not found** could mean that steering rules are not installed correctly. [PR1308884](#)
- Subscribers might not be able to access the device if dynamic VLAN is used. [PR1309770](#)
- After unified ISSU, 90 percent subscribers might downgrade from Junos OS Release 16.1 to Junos OS Release 17.3. [PR1309983](#)
- Utilization of **commit check** just after setting a master password might trigger improper decoding of configuration secrets. [PR1310764](#)
- After BSYS reboot, rpd is unresponsive sometimes on one GNFS. [PR1310765](#)
- The incorrect error number might be reported for syslog messages with a prefix of %DAEMON-3-RPD_KRT_Q_RETRIES. [PR1310812](#)
- Fragmented UDP packet might be incorrectly parsed as uBFD packet and dropped. [PR1311134](#)
- The routing protocol process (rpd) core file is generated when multiple session flap on scale setup. [PR1312169](#)
- PEM alarms and I2C failures are observed on MX240, MX480, and MX960 Series. [PR1312336](#)
- False over temperature SNMP trap could be seen when using MPC5, MPC6, MPC7, MPC8, and MPC9 on MX2020. [PR1313391](#)
- IPv6 router-solicit (RS) packets are dropped in non-default RI, for default RI it is working. [PR1313722](#)
- The CLI command **show version detail** gives severity error log **traffic-dird[20126]: main: swversion pkg: 'traffic-dird' name: 'traffic-dird' ret: 0**. [PR1313866](#)
- The mspmand process generates a core file because of the flow-control seen while clearing CGNAT+SFW sessions. [PR1314070](#)
- The MPC7E- IR-mode configuration statement commit failure. [PR1314755](#)
- The L2TP LAC might drop packets that have incorrect payload length while sending packets to the LNS. [PR1315009](#)
- Continuous logs from vhlclient for all the commands are executed. [PR1315128](#)
- The RIB and FIB might get out of synchronization because the KRT asynchronous queue might get stuck. [PR1315212](#)
- FPC crash is observed when a route has unilist next hops in RSVP scenario. [PR1315228](#)
- The CLI command **show version detail** gives severity error log **mobiled: main Neither BNG LIC nor JMOBILE package is present,exit mobiled**. [PR1315430](#)

- The output from **show configuration <> | display json** might not be properly enclosed in double quotes. [PR1317223](#)
- Linux-based micro-kernel might panic because of the concurrent update on mutable objects. [PR1317961](#)
- CoA shaping rate is not applied successfully after ISSU while doing ISSU from Junos OS Release 15.1R6.7 to 16.1R6.2. [PR1318319](#)
- The daemon bbe-smgd might crash after performing GRES [PR1318528](#)
- FPC crashes on configuration change for Packet Forwarding Engine sensors. [PR1318677](#)
- The MPC with specific failure hardware might impact other MPCs in the same chassis. [PR1319560](#)
- Kernel might generate a core file if a configuration is using more than 256 routing instances. [PR1319781](#)
- The task replication might not be complete to certain network protocols after multiple GRES. [PR1319784](#)
- Loading xmlproxy YANG files cause telemetry session and some daemons to restart. [PR1320211](#)
- Chassis MIB SNMP OIDs for VC-B member chassis are not available after MX Series Virtual Chassis unified ISSU. [PR1320370](#)
- The CLI **show subscriber summary** command displays incorrect terminated subscriber count. [PR1320717](#)
- PPP inline keepalive does not work fine as expected when CPE aborts the subscriber session. [PR1320880](#)
- MX Series routers sends the IPv6 router advertisements and the DHCPv6 advertisements before sending IPCPv6 ACK from CPE. [PR1321064](#)
- MX Series Virtual Chassis CoS is not applied to Packet Forwarding Engine when VCP link is added. [PR1321184](#)
- The bbe-smgd process generates a core file after massive clients logout and login in PPPoE dual stack subscriber scenario. [PR1321468](#)
- There is CoA-NAK with "Error-Cause = Invalid-Request" sent back to RADIUS server if applying drop policy under RADIUS-flow-tap in L2TP subscriber scenario. [PR1321492](#)
- In commit fast-synchronize mode, the commit operation might get stuck after the **commit check** is performed. [PR1322431](#)
- The rpd might crash when two next hops are installed with the same next hop index. [PR1322535](#)
- The rpd might crash when OpenConfig package is upgraded with JTI streaming data in the background. [PR1322553](#)
- [SIRT] Junos OS: MPC7E/8E/9E, PTX5K-FPC3 (FPC-P1, FPC-P2), PTX3K-FPC3 and PTX1K: Line card may crash upon receipt of specific MPLS packet (CVE-2018-0030). [PR1323069](#)
- The CLI command **request vmhost halt routing-engine other** does not halt the backup Routing Engine. [PR1323546](#)
- IS-IS fails to establish because of packets dropping on Packet Forwarding Engine. [PR1325311](#)
- A few show commands were issued twice when request support information is executed. [PR1327165](#)

- MS-MIC interface logical interfaces remain down after many iterations of offline or online. [PR1322854](#)
- NCP Conf-Ack or Conf-Req packets might be dropped constantly from Cisco MLPPP client on Tomcat. [PR1323265](#)
- CLI commands in **show system subscriber-management route routing-instance <xxx>** hierarchy show unexpected outputs. [PR1323279](#)
- Memory leaks in MGD-API daemon during get API requests and error handling during set API request. [PR1324321](#)
- Subscribers might fail to login after the interface is deactivated or activated. [PR1324446](#)
- The memory leakage is seen in mosquito-nossl daemon. [PR1324531](#)
- The SNMP interface filter does not work when "interface-mib" is part of dynamic-profile. [PR1324573](#)
- The VLAN re-write function might put incorrect VLAN-id when Ethernet OAM is configured on DPCE cards. [PR1325070](#)
- SNMP values might not be increased monolithically. [PR1325128](#)
- MPC cards might drop traffic under high temperature. [PR1325271](#)
- The VLAN DEMUX interface does not respond the ARP request in subscriber scenario with MX Series after Junos OS Release 15.1 with subscriber management enabled. [PR1326450](#)
- In MX Series BNG CoS service object is not deleted properly for TCP and scheduler. [PR1326853](#)
- An incorrect output is observed while verifying the command **show subscribers client-type vlan subscriber-state active logical-system default routing-instance default**. [PR1322907](#)
- Minor alarm **LCM Peer Connection un-stable** is observed on MX150 after the chassisd process startup or restart. [PR1328119](#)
- The following logs repeat every 5 seconds in chassisd log: **fm_feacap_sys_feature_get:Attribute DB init not yet done, reading from pvid (id: 18), fm_feacap_sys_feature_get: Attribute key fabric.planes_per_board does not exists**. [PR1328868](#)
- When an AMS bundle has a single MAMs added to it, the subinterfaces do not recover after the subinterface has been disabled. [PR1329498](#)
- Host-Outbound traffic is not rewriting ieee-801.pbits for dynamic subscriber logical interface over PS interface. [PR1329555](#)
- SNMP walks of interfaces related MIB objects are slower than expected in a scaled configurations. [PR1329931](#)
- The statement **show services nat mappings address-pooling-paired** times out and fails. [PR1330207](#)
- An rpd core file is generated on a new backup Routing Engine at **task_quit,task_terminate_timer_callback,task_timer_dispatch,task_scheduler** after disabling NSR+GRES. [PR1330750](#)

- Too many supplies missing in lower or upper zone alarm flap (set/clear) every 20 seconds if a zone does not have minimum required PSMs. [PR1330720](#)
- All packets might be dropped if one route is adverted by BGP which session is established through the subscriber interface. [PR1330737](#)
- FPC wedge with fragmented packets on LSQ interface - PT1: Head and Tail out of synchronization. [PR1330998](#)
- Chassis FPC temperature with non-nebs optics higher after software upgrade. [PR1331186](#)
- The bbe-smgd process might crash after executing the command of **clear ancp access-loop circuit-id <circuit-id>**. [PR1332096](#)
- The rpd core file generated might be seen in l2circuit or l2vpn environment. [PR1332260](#)
- Inaccurate J-Flow records might be seen for output interface and next hop. [PR1332666](#)
- On MX150 platform **set chassis alarm management-ethernet link-down ignore** not an ignoring alarm for FPC Mgt 0 interface. [PR1332799](#)
- The dot1xd might crash if ports in multi-suppllicant mode flap. [PR1332957](#)
- The subinfo process might crash and it might cause the PPPOE subscribers to get disconnected. [PR1333265](#)
- The MX Series routers might not be able to learn the global IPv6 neighbor address of its DHCPv6 subscriber client. [PR1333392](#)
- JDID thrashes continuously and continuous log messages are observed in syslog. [PR1333632](#)
- The l2ald process generates a core file on EVPN-VXLAN network. [PR1333823](#)
- AA EVPN VXLAN high CPU on backup routing protocol process(rpd). [PR1334235](#)
- Two subscribers cannot reach the online state at the same time if they have an identical frame-route attribute value. [PR1334311](#)
- windsurf card went for "restart" post ISSU to Junos OS Release 18.2DCB in MX2010 box. [PR1334612](#)
- The ffp crash might be seen when execute software upgrade (non-ISSU). [PR1334745](#)
- The rpd crashes when performing the BGP configuration change. [PR1334846](#)
- The UID limit is reached in large-scale subscriber scenario. [PR1334886](#)
- When using **show subscribers** and FPC number has two digits, the interface and IPv6 address get connected together for DHCPv6 PD. [PR1334904](#)
- MQSS errors and alarms might happen with interface going down. [PR1334928](#)
- IPsec SA cfg name mismatch and cfg could not be pushed to PIC. [PR1334966](#)
- Traffic drops on the MX Series LNS because of the software error or unknown family exception when traffic destined to or coming from MLPPP subscriber if **routing-services** configuration statement is present in the dynamic-profile used by this subscriber. [PR1335276](#)

- On MX Series platforms, 3RU master LED glows on master and backup RCB, while performing the image upgrade on master with GRES/NSR enabled. [PR1335514](#)
- The RIP route updates might be partially dropped when NSR is enabled. [PR1335646](#)
- The MAC_STUCK might be seen on MS-MPC or MS-MIC. [PR1335956](#)
- JET application might not respawn after a normal exiting. [PR1336107](#)
- Subscriber might experience SDB DOWN event and drop the clients' connections when issuing **show subscribers** command. [PR1336388](#)
- On MX2000 with SFB card installed, high amount of traffic volume on MPC7E, MPC8E or MPC9E might cause traffic drops with cell underflow messages. [PR1336446](#)
- The hash value generated for 256-bit key length of AES-GCM-256 algorithm is incorrect. [PR1336834](#)
- BBE-SMGD might core when doing CoS configure of ifl-set. [PR1336852](#)
- Configuring **lldp neighbour-port-info-display port-id** does not take any effect. [PR1336946](#)
- Error log message **sdb_db_interface_remove: del ifl:si-<index> with licnese cnt non-zero on** can be seen on LTS during subscriber logout. [PR1337000](#)
- AI-script does not get auto re-install upon a Junos OS upgrade on next-generation Routing Engine. [PR1337028](#)
- DDoS counters for OSPF might not increase. [PR1339364](#)
- The MX10003 MPC off-line button is not effective. [PR1340264](#)
- Very few of subscribers show incorrect accounting values in large-scale subscribers scenario. [PR1340512](#)
- VRRP stuck in master on upgrade or cold boot. [PR1341044](#)
- There might be a traffic loss on some subscriber sessions when more than 32K L2TP subscriber sessions are anchored in ASI interface. [PR1341659](#)
- The reboot of Routing Engine might occur if PPPoE interface is configured over an aggregate Ethernet or RETH interface. [PR1341968](#)
- With discard interfaces configured with IGMPv3, KRT queue get stuck while deleting multicast next hop (MCNH) with an error **EPERM -- Jtree walk in progress**. [PR1342032](#)
- jnxContentsType does not display details related to fixed ports and normal TIC. [PR1342285](#)
- SNMP walk might failed for LLDP related OIDs. [PR1342741](#)
- The vFPC might get absent resulting in the total loss of traffic. [PR1343170](#)
- Support required for **show system resource-monitor subscribers-limit chassis extensive** command in summit. [PR1343853](#)
- The 100M SFP is not from Fiberxon or Avago and might not work on MIC-3D-20GE-SFP-E and MIC-3D-20GE-SFP-EH. [PR1344208](#)

- MX Series router is sending IPv6 RA and the DHCPv6 advertisements before IPCPv6 Ack from CPE. [PR1344472](#)
- Unable to route over RLT interface post upgrading from Junos OS Release 15.1 to Junos OS Release 17.3. [PR1344503](#)
- On Junos OS Release 18.2, the ancpd process generates a core file at `src/junos/usr.sbin/ancpd/ancpd_smgd.c:2299` in clearing ancp subscribers in a scaled scenario. [PR1344805](#)
- The framed-route "0.0.0.0/0" will not be installed in MX Series platform with Junos OS enhanced subscriber management releases. [PR1344988](#)
- In EVPN-VXLAN, ARP packet uses VRRP/virtual-gateway MAC in Ethernet header instead of IRB MAC address. [PR1344990](#)
- CPCD process generates a core file because the converged services support for Routing Engine-based captive portal is used. [PR1345096](#)
- On any product supporting dot1x, as part of authentication of a VOIP phone, its MAC address gets added in both voice and data VLANs. If traffic is received only on the voice VLAN, the MAC address gets aged-out from the data VLAN and due to this the session gets cleared. [PR1345365](#)
- The routing protocol process (rpd) might if **no-propagate-ttl** configuration statement is set in a routing instance which has a specific route. [PR1345477](#)
- MAC address of multiple interfaces are found to be duplicate. [PR1345882](#)
- Routing Engine model changed from JNP10003-RE1 to RE-S-1600x8. [PR1346054](#)
- New PPPoE users might fail to login. [PR1346226](#)
- **AC system error** counter in **show pppoe statistics** is not working. [PR1346231](#)
- VCCP-ADJDOWN detection is delayed on VC-Bm when deleting one vcp link on VC-Mm. [PR1346328](#)
- Statistics daemon pfed might generate a core file on an upgrade between certain releases. [PR1346925](#)
- twice-napt-44 sessions not synchronizing to backup SDG with **stateful sync** configured. [PR1347086](#)
- IPv6 MAC resolve fails if the DHCPv6 client uses a non-EUI64 link-local address. [PR1347173](#)
- Issue with handling the community_action ("add") in RPC call. [PR1348082](#)
- The FPC might crash due to MIC error interrupt hogging. [PR1348107](#)
- Packet loop is detected when vrf multipath is enabled with **equal-external-internal** configuration statement under L3VPN instance and install-nexthop is enabled in forwarding table export policy regarding that L3VPN route. [PR1348175](#)
- Chassisd memory leak issue on MX10003 and MX204 platform and it would cause eventual Routing Engine switchover and crash. [PR1348753](#)

- DHCPv6 Solicit dropped on L2TP LNS in MX Series Virtual Chassis when incoming interface is on VC-master and both anchor si-interface and VCP port on VC-backup on MPC2 NG or MPC2 NG. [PR1348846](#)
- The dcd process might crash after any other smid related daemon crashes. [PR1349154](#)
- A major alarm: "Major PEM 0 Input Failure" might be observed for DC PEM. [PR1349179](#)
- The mspmand process might crash when executing **show services nat deterministic-nat nat-port-block** command. [PR1349228](#)
- The pccd might crash after a delegated LSP is removed in PCEP scenario. [PR1350240](#)
- Multicast traffic gets dropped as invalid policy ID exception. [PR1350380](#)
- The MTU value for subscriber's interface might be programmed incorrectly if the configuration statement **routing-services** or **protocol pim** is configured in dynamic profile. [PR1350535](#)
- The VCP port might not come back up after removing and adding it again. [PR1350845](#)
- The subinfo process might crash when executing **show subscribers address <> extensive** for a DHCPv6 address. [PR1350883](#)
- The pfed process consuming 80-90% CPU running subscriber management on PPC based routers. [PR1351203](#)
- The high CPU usage of bbe-smgd process might be seen when L2BSA subscribers get stuck. [PR1351696](#)
- After GRES, the BGP neighbors at master Routing Engine might reset and the BGP neighbors at backup Routing Engine take long time to establish. [PR1351705](#)
- Bbe-smgd process (daemon) might restart in subscriber environment. [PR1352546](#)
- The DHCP relay-reply packets are dropped in the DHCPv6 relay scenario. [PR1352613](#)
- The offline MIC6-100G-CFP2 MIC through the CLI command might trigger FPC card to crash. [PR1352921](#)
- The routing protocol process (rpd) permanently hogs CPU because of the logical system configuration commit. [PR1353548](#)
- Flabels might get exhausted after multiple Routing Engine switchover. [PR1354002](#)
- A syslog error **dfw_bbe_filter_bind:1125 BBE Filter bind type 0x84 index 167806251 returned 1** might occur [PR1354435](#)
- The rpd generates core files that is seen when adding an inter-region template in routing instances. [PR1354629](#)
- Aggregated Ethernet operational state goes up even though some of the member interfaces configured under the aggregate Ethernet are down. [PR1354686](#)
- The ifinfo process could crash in MX Series router BNG running L2BSA service. [PR1354712](#)
- A memory leak found in agentd when running valgrind. [PR1354922](#)
- The fabric chip failure alarms are observed in GRES scenario. [PR1355463](#)

- The following syslog messages are seen: **ui_client_connect_to_kmd_instance: KMD-SHOW connect to kmd-instance failed kmd-instance RE, fpc slot 0, pic slot 0.** [PR1355547](#)
- The rpd crashes when CLI **show dynamic-tunnels database terse** is executed when system have RSVP tunnels configured. [PR1356254](#)
- I2c messages from PEM or PSM are reported if SNMP is enabled. [PR1356259](#)
- DHCP subscribers fail after reconfiguration of port from tagged to un-tagged mode. [PR1356980](#)
- Routing Engine switchover during backup Routing Engine being not GRES ready might restart the linecard. Routing Engine kernel and multiple chassisd might crash. [PR1357427](#)
- MX Series Virtual Chassis locality bias with random ECMP, multipath vpn-unequal-cost and unique aggregated Ethernet bundles on each member. The traffic incorrectly hashes on both the aggregated Ethernet interfaces. [PR1358635](#)
- MPCs might restart during a unified ISSU. [PR1359282](#)
- Routes stuck in KRT queue with an error **EINVAL -- Bad parameter in request.** ' [PR1362560](#)
- A memory leak in bbe-smgd might be observed if dynamic profile variable name and the associated value is configured to be same. [PR1362810](#)
- Traffic destined to the MAC/IP address of VRRP VIP get dropped on the platforms which have common TFEB terminals such as MX5, MX10, MX40, MX80, and MX104. [PR1363492](#)
- A traffic loop might occur even though the port is blocked by RSTP in a ring topology. [PR1364406](#)
- The traffic is still forwarded through the member link of an aggregated Ethernet bundle interface even with "Link-Layer-Down" flag set. [PR1365263](#)
- The next hop of MPLS path might be stuck in hold state which could cause traffic loss. [PR1366562](#)

High Availability (HA) and Resiliency

- After flapping server CB ports GNFs shows **Switchover Status: Not Ready.** [PR1306395](#)
- The ksyncd process might crash continuously on the new backup Routing Engine after performing GRES. [PR1329276](#)
- Insufficient available space on hard disk lead by the crash information files is generated by ksyncd when GRES is configured in large scale configuration scenario. [PR1332791](#)

Infrastructure

- A use-after-free vulnerability exists in rpcbind of Juniper Networks Junos OS allows an attacker to cause a denial of service against rpcbind. [PR1188676](#)
- On Junos OS, kernel crash (vmcore) during broadcast storm after enabling 'monitor traffic interface fxp0' (CVE-2018-0029). [PR1322294](#)
- Cleanup at thread exit cause memory leaks. [PR1328273](#)

- On all Junos OS platforms, on a port configured with both dot1x static MAC by-pass and normal authentication, the hosts configured for static MAC by-pass might not be able to send traffic. [PR1335125](#)
- The kernel might crash and the system might reboot in SNMP query reply scenario. [PR1351568](#)
- Junos OS no longer going to db prompt at ~ + ctl-b. [PR1352217](#)

Interfaces and Chassis

- On MX240, MX480, and MX960 IPv6 neighborship is not created on IRB interface. [PR1198482](#)
- Identical IP address can be configured on different logical interfaces from different physical interfaces in the same routing instance (including master routing instance). [PR1221993](#)
- RL-dropped packets are not displayed by [**show interfaces <ifl-or> detail/extensive**] commands. [PR1249164](#)
- L2TP subscribers might not be cleared if the access-internal routes fail to install. [PR1298160](#)
- No route to IP address from directly connected route. [PR1318282](#)
- If ultra forward error correction (UFEC) with optical transport network (OTN) is configured, and the physical link goes down, CPU will go to 100 percent. If UFEC with OTN is configured on unconnected interfaces, CPU will go to 100 percent. [PR1311154](#)
- The command **show interfaces interface-set** displays incorrect logical interface. [PR1319682](#)
- IPCP negotiation might fail for dual stack PPPoE subscribers. [PR1321513](#)
- Unexpected log messages might be seen if a BGP session flaps in a dynamic-tunnels GRE scenario. [PR1326983](#)
- Unexpected log messages might be seen on a router for subscriber management. [PR1328251](#)
- Traffic loss might be seen after deleting aggregated Ethernet bundle unit 1. [PR1329294](#)
- The cfmd process generates a core file. [PR1329779](#)
- The interface might not work properly after FPC restarts. [PR1329896](#)
- The dcd process might crash because of the memory leak causing commit failure. [PR1331185](#)
- The last logical interface digit sometimes truncate in jpppd trace logs. [PR1332483](#)
- The transportd might crash when an SNMP query on jnxoptIfOChSinkCurrentExtTable with unsupported interface index. [PR1335438](#)
- MX Series routers might occasionally drop the first LCP configure request packet when operating in PPPoE subscriber management configuration. [PR1338516](#)
- Suppressing cfmd logs : jnxSoamLmDmCfgTable_next_lookup: md 0 ma 0 md_cfg 0x0 [PR1347650](#)
- The jpppd process generates a core file on backup Routing Engine in longevity test at `../../../../../../../../src/junos/usr.sbin/jpppd/pppMain.cc:400`. [PR1350563](#)

- The FPC might be stuck at 100 percent for long time when MC-AE with enhanced-convergence is configured with large-scale logical interfaces. [PR1353397](#)
- Clients might not get IPv4 address in PPPoE dual-stack scenario. [PR1360846](#)

Layer 2 Ethernet Services

- DHCPv6 traffic might be dropped in subscriber scenario. [PR1316274](#)
- The jdhcpd process generates a core file after making DHCP configuration changes. [PR1324800](#)
- The on-demand-address-allocation under dual-stack-group does not work for IPv6. [PR1327681](#)
- The snmpget for OID: dot3adInterfaceName might not work. [PR1329725](#)
- The memory leak might occur in l2cpd if the l2-learning process is disabled. [PR1336720](#)
- On Junos OS, a malicious crafted IPv6 DHCP packet might cause the jdhcpd process to generate a core file(CVE-2018-0034). [PR1334230](#)
- The jdhcpd process might spike to 100% from less than 10% when DHCPv6 is used. [PR1334432](#)
- The DHCPv6 second solicit message might not be processed when IA_NA and IA_PD are sent in a separate solicit message. [PR1340614](#)
- DHCP client is not able to connect if VLAN was modified on the aggregated Ethernet interface associated with the IRB. [PR1347115](#)
- ZTP infra scripts are not included for MX Series PPC routers. [PR1349249](#)
- When DHCP subscribers are in bound (LOCAL_SERVER_STATE_WAIT_GRACE_PERIOD) state if dhcp-service is restarted then the subscribers in this state are logged out. [PR1350710](#)
- DHCP relay agent will discard DHCP request message silently if the requested IP address has been allocated to the other client. [PR1353471](#)
- Restart FPC which homing micro-bfd link causing lacp to generate a core file. [PR1353597](#)
- The DHCP lease query message is replied with incorrect source address. [PR1367485](#)

Layer 2 Features

- The rpd process memory leak is observed upon any changes in VPLS configuration like deleting or re-adding VPLS interfaces. [PR1335914](#)
- VPLS instance stays in NP state after LDP session flaps [PR1354784](#)

MPLS

- The ingress RSVP LSP fails to come UP after **clear rsvp lsp** all on egress router. [PR1275563](#)
- The rpd might crash in LDP Layer 2 circuit scenario. [PR1275766](#)
- When an LDP egress policy is used for inet.3 BGP labeled-unicast route, the route label might not be installed in the Label Distribution Protocol (LDP) database. [PR1289860](#)

- The traffic drop during NSR switchover for RSVP P2MP provider tunnels used by MVPN. [PR1293014](#)
- The process rpd might crash when performing MPLS traceroute. [PR1299026](#)
- The traffic in P2MP tunnel might be lost when next-generation MVPN uses RSVP-TE. [PR1299580](#)
- The kysncd process might crash after removing and inserting backup Routing Engine in analytics and "mpls sensor" scenario. [PR1303491](#)
- The RSVP node-hello packet might not work correctly after the next hop for remote destination is changed. [PR1306930](#)
- When **show mpls container-lsp** is executed, the output is delayed. [PR1314960](#)
- With **dynamic-tunnels** configured, the rpd might crash when the rpd is restarted or Routing Engine switchover is executed. [PR1319386](#)
- The IPv4 and IPv6 multicast traffic might get dropped in MX Series Virtual Chassis when the traffic comes in through the layer 2 circuit and goes out through aggregated Ethernet member interface across Virtual Chassis members. [PR1320742](#)
- The rpd might crash when ldp p2mp recursive is configured. [PR1321626](#)
- The rpd might crash due to memory leak in RSVP scenario. [PR1321952](#)
- On Junos OS, receipt of specially crafted UDP packets over MPLS might bypass stateless IP firewall rules (CVE-2018-0031). [PR1326402](#)
- SNMP OID counters for mplsLspInfoAggrOctets show constant value for some LSPs even though traffic is constantly increasing in **show mpls lsp statistics**. [PR1327350](#)
- Packet loss might be observed when auto-bandwidth is enabled for CCC connections. [PR1328129](#)
- The rpd might crash on backup Routing Engine because of memory exhaustion. [PR1328974](#)
- After a MPLS LSP link flap and local repair, a new LSP instance is tried to be signaled but it might get stuck. [PR1338559](#)
- Whenever there is a decrease in the statistics value across an LSP, the mplsLspInfoAggrOctets value take two intervals to get updated. [PR1342486](#)
- LDP label is generated for serial interface subnet route unexpectedly. [PR1346541](#)
- The rpd crash might happen in RSVP setup-protection scenario. [PR1349036](#)
- In a rare scenario, rpd might crash when LDP fails to allocate self-id for the P2MP FEC. [PR1349224](#)
- Packets destined to the master Routing Engine might be dropped in the kernel when LDP traffic statistics are polled through SNMP. [PR1359956](#)

Multicast

- DHCP6 relay is not working unless DHCP is restarted. [PR1316210](#)
- Incorrect upstream interface might be displayed on PIM non-DR router for some statically joined IGMP groups. [PR1337591](#)

Network Management and Monitoring

- On MX Series virtual devices, one Routing Engine does not reply to SNMP request. [PR1240178](#)
- The alarm-mgntd might crash after upgrade to Junos OS Releases 16.1R4, 16.1R5, 17.1R3, 17.2R1, 17.3R1, or later releases. [PR1296597](#)
- The mib2d might crash when SNMP polling on interface mibs and meanwhile FPC restarts or interface flaps. [PR1318302](#)
- SNMP stops or becomes very slow after a very long period of time. [PR1328455](#)
- With **interafce-mib**, MX Series routers responds with **type : NoSuchInstance** for OIDs when multiple OIDs are polled in one SNMPGET request. [PR1329749](#)
- The eventd process fails to startup with syslog configuration. [PR1353364](#)
- **jnxDcuStatsEntry** and **jnxScuStatsEntry** OIDs are missing post interface configuration change. [PR1354060](#)
- SNMP process crashes during CFM statistics polling. [PR1364001](#)

Platform and Infrastructure

- On MX Series platforms, if a large number of routes are processed, then the Packet Forwarding Engine of the MS-MPC might crash. [PR1277264](#)
- Error messages might be observed with MPC5E card. [PR1283850](#)
- Executing the command of **show services inline ip-reassembly statistics** might cause ukern sheaf memory leak. [PR1285833](#)
- The output values of command **show system resource-monitor** are not accurate. [PR1287592](#)
- Doing load replace terminal and attempting to replace the interface stanza might terminate the current CLI session and leave the user session hanging. [PR1293587](#)
- Service cookie opaque data reset incorrectly leading data sent to service pic getting corrupted. [PR1310904](#)
- VPLS instance fails to learn MAC addresses upon pseudowire switchover. [PR1316459](#)
- Rate-limit configured with small temporal buffer size might cause packet loss. [PR1317385](#)
- Multicast traffic might get duplicated when MoFRR is configured. [PR1318129](#)
- Move XQ_CMERROR_XR_CORRECTABLE_ECC_ERR to minor and re-classify remaining XQCHIP CMERROR from FATAL to MAJOR. [PR1320585](#)
- The traffic with more than 2 VLAN tags might be incorrectly rewritten and sent out. [PR1321122](#)
- MX104 shows **sdk-vmmd: %USER-3: is_platform_rainier: Platform could not be detected** in severity error. [PR1321622](#)
- The 'no-propagate-ttl' might not take effect if **chained-composite-next-hop ingress l3vpn extended-space** is configured. [PR1323160](#)
- The MAC might not be learnt on MX Series with MPCs or MICs line card because of the negative value of the bridge MAC table limit counter. [PR1327723](#)

- The packet might get dropped in LSR if MPLS pseudowire payload does not have control word and its destination MAC starts with '4' or '6'. [PR1327724](#)
- Traffic loss might be observed on LT interface. [PR1328371](#)
- Directories and files under `/var/db/scripts` lost execution permission or directory 'jet' is missing under `/var/db/scripts` causing **error: Invalid directory: No such file or directory** error during commit. [PR1328570](#)
- The tcpdump filter might not work in egress direction on PS and its logical interfaces. [PR1329665](#)
- The router hits db prompt at `netisr_process_workstream_proto`. [PR1332153](#)
- RPM mib `pingResultsMinRtt`, `pingResultsMaxRtt`, `pingResultsAverageRtt` response as "1" while target address is unreachable, should be "0". [PR1333320](#)
- On all Junos OS platforms, python scripts and shell scripts cannot be executed during ZTP as `verixec` is enabled. [PR1334425](#)
- Traffic loss might be seen for some flows due to network churn. [PR1335302](#)
- Commit might fail with error reading from commit script handler. **error: commit script failure** [PR1335349](#)
- On MX104, a backup Routing Engine kernel crashes on committing **set system management-instance**. [PR1335903](#)
- The MPC might crash after setting max-queues to a very large number. [PR1338845](#)
- On MX Series platform with network services in IP mode and Connectivity Fault Management (CFM) configured on aggregated Ethernet interface, route programming in Packet Forwarding Engine might get corrupted after the member link of aggregated Ethernet flap, leading to packet drop. [PR1338854](#)
- Configuring the same DHCP server in different routing instances is not supported in DHCP relay scenario. [PR1342019](#)
- With **proxy-arp** configuration statement present on a VRRP interface transition of VRRP backup to master might result in dead next hops. [PR1342707](#)
- Packet Forwarding Engine route might get corrupted post few attempts of deactivation or activation of CFM feature list either through interface flap or restart of FPC hosting the member links aggregated Ethernet with CFM configured leading to packet black-holes. [PR1342881](#)
- ZTP is not supported for vmhost images on next generation Routing Engines on the MX Series platforms. [PR1343338](#)
- On Junos OS, multiple vulnerabilities in multiple cURL versions are seen. [PR1347361](#)
- The IPv4 GRPS traffic over aggregated Ethernet interface might be dropped if **gtp-tunnel-endpoint-identifier** is configured. [PR1347435](#)
- On an EVPN-VXLAN, MX Series output policing action does not work on IRB interfaces for VNIs. [PR1348089](#)
- FPC CPU utilization with LT interfaces is pegged continuously at 100 percent. [PR1348840](#)
- Running RSI through console port might cause system to crash and reboot. [PR1349332](#)

- ICMP error messages are not generated if 'donot fragment' packets exceed the MTU of the multiservice interface. [PR1349503](#)
- Kernel crashes because of the initialization of logical interface MAC filter function missing for Packet Forwarding Engine extended port devices. [PR1353498](#)
- JNH memory leak is seen with VTEP traffic. [PR1356279](#)
- Traffic black hole seen along with JPRDS_NH:jprds_nh_alloc(),651: JNH[0] failed to grab new region for next hop messages. [PR1357707](#)

Routing Policy and Firewall Filters

- Condition based policy fails to take action even though condition is matched. [PR1300989](#)
- The policy configuration might not be evaluated if policy expression is changed. [PR1317132](#)
- Access internal route might fail to be leaked between routing instances when **from instance** is configured in the policy. [PR1339689](#)
- TPI-50840 vrf-target auto derived internal policy not cleaned up even after configuration is deleted and triggers rpd to generate a core file. [PR1357724](#)

Routing Protocols

- The CLI command **show bgp summary** provides incorrect results while assisting GR. [PR1045151](#)
- The rpd might crash when running rpd for a long time. [PR1092009](#)
- RLFA computation might still consider a PQ-node not reachable through LDP, when LDP is deactivated. [PR1202392](#)
- BGP extended communities with sub-type 4 erroneously displayed at LINK_BANDWIDTH. [PR1216696](#)
- The rpd generates a core file in the ASBR when BGP is deactivated in the ASBR before all stale labels have been cleaned up. [PR1233893](#)
- After bfdd restart is seen, issue with next-generation mVPN and l2vpn route exchange causes mVPN and vpls traffic drop. [PR1278153](#)
- Routing loops might be seen after configuring BGP prefix independent convergence (BGP PIC). [PR1282520](#)
- Multicast flow reset might occur on OIF for RPT joined branch when PIM prune comes on another interface. [PR1293900](#)
- The link management protocol process (Impd) repeatedly crashes when a logical system is configured on the same router. [PR1294166](#)
- The rpd process might crash because of the AS PATH check error that occurs when RIB groups are added first and later the routing instances are added. [PR1298262](#)
- MSDP sessions might flap because the data replication get stuck between backup and master Routing Engine with a huge SA burst between peers. [PR1298609](#)

- The rpd might crash because of the malformed BGP UPDATE packet (CVE-2018-0020). [PR1299199](#)
- IBGP route damping does not take effect on IBGP inet-vpn address family. [PR1301519](#)
- Multicast traffic might be pruned for random groups following DR failover. [PR1303050](#)
- The mcsnoopd process generates a core file at `__raise,abort,__task_quit__,task_quit,task_terminate_timer_callback,task_timer_dispatch,task_scheduler_internal(enable_slip_detector=true,no_exit=true)` at `../src/junos/lib/libtask/base/task_scheduler.c:275`. [PR1305239](#)
- BGP traceoption logs are still written when it is deactivated. [PR1307690](#)
- The rpd generates a core file in `bgp_rt_send_message` at `../src/junos/usr/sbin/rpd/bgp/bgp_io.c:1460`. [PR1310751](#)
- BGP route age is getting refreshed when secondary path goes down with BGP PIC enabled. [PR1312538](#)
- The routing protocol process (rpd) might crash and generate core files. [PR1314679](#)
- The rpd might constantly consume high CPU in BGP setup. [PR1315066](#)
- OSPF routes cannot be installed to the routing table until the lsa-refresh timer expire. [PR1316348](#)
- The primary path of MPLS LSP might switch to other address. [PR1316861](#)
- The inactive route cannot be installed in multipath next hop after disabling and enabling the next hop interface in L3VPN scenario. [PR1317623](#)
- The MPLS labels next hop for IPv4 labeled unicast route are incorrect while doing some changes to the active LDP route. [PR1317800](#)
- IS-IS might choose a sub-optimal path after the metric change in ECMP links. [PR1319338](#)
- Traffic might get silently dropped and discarded temporarily when BGP GR is triggered and the direct interface flap. [PR1319631](#)
- Issue with tracing of the BGP L2VPN DF election community. [PR1323596](#)
- The rpd crash is seen when deactivating static route if the next hop interface is type of P2P. [PR1323601](#)
- When a prefix limit is reached, increasing maximum prefixes does not take effect. [PR1323765](#)
- BGP peer is not established after Routing Engine switchover when graceful restart and BFD is enabled. [PR1324475](#)
- The rpd process might crash continuously on both Routing Engines when **backup-spf-options remote-backup-calculation** is configured in IS-IS protocol. [PR1326899](#)
- Multiple next hops might not be installed for IBGP multipath route after IGP route update. [PR1327904](#)
- The OpenSSL project has published a security advisory for vulnerabilities resolved in the OpenSSL library on December 7, 2017. This issue might be seen if SSL service is used, like J-Web (HTTPs), SSH, etc. [PR1328891](#)
- With BGP, LDP, and IS-IS configurations, deleted IS-IS routes might still be visible in RIB. [PR1329013](#)

- The rpd might crash on backup Routing Engine after BGP peer is deleted. [PR1329932](#)
- Manual GRES with MX Series Virtual Chassis results in some packet loss on core facing interfaces. [PR1329986](#)
- The conditional route policy cannot withdraw all routes in BGP add-path scenario on vMX platform. [PR1331615](#)
- LDP route in inet.3 is missing when both OSPF rLFA and LFA protections are available and rejected by backup selection policy. [PR1333198](#)
- With introduction of PR1282672, discard nh being installed when primary LSP interface drops. When primary interface returns, discard nh remains until BGP LU neighbor is cleared. This only impacts the cloned route (S=0). [PR1333570](#)
- In LI, IGMP joins are not processed with **passive allow-receive** statement configured on IGMP interface. [PR1334913](#)
- BGP sessions get stuck in active state after remote end (Cisco) restart the device. [PR1335319](#)
- The rpd might crash if SRLG information is in the protocol IS-IS. [PR1337849](#)
- The rpd crash might occur when receiving BGP updates. [PR1341336](#)
- The mcsnoopd process might lead to a memory leak. [PR1326410](#)
- The igmp-snooping might be enabled unexpectedly. [PR1327048](#)
- On Junos OS, the rpd crashes while receiving a crafted BGP UPDATE. [PR1327708](#)
- The routing protocol process (rpd) might crash due to receipt of crafted BGP notification messages. [PR1340689](#)
- Changes to the displayed value of AIGP in **show route ... extensive** command. [PR1342139](#)
- Traffic black-hole might be seen if local DUT receiving BFD is down. [PR1342328](#)
- The rpd might crash when deleting or deactivating the VRF routing instance in BGP Layer 3 VPN environment. [PR1343578](#)
- The rpd might crash if a route for RPF uses a qualified-next-hop. [PR1348550](#)
- Traffic loss might be seen after the upstream interface shifts from one to another during receiving the PIM prune packet. [PR1350806](#)
- The rpd might crash when BGP route damping and BGP multipath features are configured. [PR1350941](#)
- The source-as community is not appended to RP (display issue in **show route** detail output). [PR1353210](#)

Services Applications

- PCP mappings cannot be manually cleared when a NAT pool is shared between PCP and standard NAT. [PR1284261](#)
- AVP 145 is not present in IRQ when ANCP DSL-type = 0. [PR1313093](#)

- L2TP Tunnel Tx and Rx bytes count sometimes decrease when subscriber sessions are reduced within the tunnel. [PR1318133](#)
- SNMP MIBs do not yield data related to sp interfaces. [PR1318339](#)
- The MRU might be changed to 1492 instead of the default 1500 in L2TP scenario. [PR1319252](#)
- Long route remains in forwarding table after subscriber session goes down. [PR1322197](#)
- L2TP LTS might drop the first "CHAP Success" packet from LNS because of delayed programming of /136 route on Packet Forwarding Engine. [PR1325528](#)
- The jl2tpd might crash if the RADIUS server returns 32 tunnel-server-endpoints. [PR1328792](#)
- In case the number of sessions addressed in CSURQ is more than about 107, not all CSURQ messages receive a response. [PR1330150](#)
- Aborting (using Ctrl+C) two commands by using the same management socket pointer, one after the other, might result in generating a core file. [PR1337406](#)
- The CLI command **show services stateful-firewall flows count** shows incorrect flow count after services configuration change. [PR1338704](#)
- Output of **show interfaces si-x/y/z.xxxxx extensive** CLI command shows incorrect inet/inet6 MTU value for MLPPP subscriber on MX Series L2TP LNS. [PR1346049](#)
- The bbe-smgd process might crash if there are 65535 L2TP sessions in a single L2TP tunnel. [PR1346715](#)
- Session limit per tunnel on LAC does not work as expected. [PR1348589](#)
- On performing an SNMP walk on the IKE SA that is deleted, IPsec tunnels might go down and an infinite loop scenario might be seen. [PR1348797](#)
- UDP checksum inserted by MS-DPC after NAT64 is not valid when incoming IPv4 packet has UDP checksum set to 0. [PR1350375](#)
- The **show services stateful-firewall flows counter** shows ridiculously high numbers. [PR1351295](#)
- J12tpd process might crash shortly after one of L2TP destinations becomes unavailable. [PR1352716](#)

Software Installation and Upgrade

- The new versions of Junos OS does not have the tool for accessing aux port - /usr/libexec/interposer. [PR1329843](#)

Subscriber Access Management

- The IP addresses of subscribers assigned by RADIUS might be counted within local pool incorrectly after Virtual Chassis switchover. [PR1286609](#)
- Service interim missing for random users in JSRC scenario. [PR1315207](#)
- The PPPOE subscribers might encounter connection failure during login. [PR1317019](#)
- IP addresses are assigned discontinuously from the linked IP pools. [PR1323829](#)

- Authd considers RADIUS attribute Framed-IPv6-Prefix = ::/64 or Delegated-IPv6-Prefix = ::/56 as valid parameters. [PR1325576](#)
- multiple-radius-servers having different dynamic-request-port is not supported. [PR1330802](#)
- Subscriber might get stuck in terminated state when JSRC synchronize state get stuck in "FULL-SYNC in progress". [PR1337729](#)
- The rate limit of upstream or downstream values are not updated in L2TP ICCN packet after the L2TP session is established. [PR1338786](#)
- In dual stack subscribers scenario when NDRA pool is configured, the linked pools are not used when the first NDRA pool is exhausted. [PR1351765](#)
- When attempting to scale, sdbsts_lock_holder.bbe-smgd.pid10686.core generates a core file. [PR1358339](#)

User Interface and Configuration

- CLI session might die while issuing the command **show configuration | compare rollback 1**. [PR1331716](#)

VPNs

- In a specific CE device environment in which asynchronous-notification is used, after the link between the PE and CE devices goes up, the L2 circuit flap repeatedly. [PR1282875](#)
- Un-hide **set protocols pim mvpn family inet6 disable** configuration to allow users to disable inet6 on mvpn. [PR1317767](#)
- The rpd might crash after unified ISSU in a large scale scenario with PIM configuration. [PR1322530](#)
- Moving MC-LAG from LDP-based pseudowire to BGP-based pseudowire might cause rpd to crash. [PR1325867](#)
- The multicast might be rejected when Junos OS PE devices received C-Mcast route from other vendors' PE devices. [PR1327439](#)
- **mvpn sender-site** configuration is not allowed with S-PMSI. [PR1328052](#)
- In a next generation MVPN and NSR configuration, the rpd process might crash and generate a core file on the backup Routing Engine. [PR1328246](#)
- The rpd might continuously crash on the backup Routing Engine and some protocols might flap on the master Routing Engine if **hot-standby** is configured for I2circuit or VPLS backup-neighbor. [PR1340474](#)
- The rpd might crash on backup Routing Engine when changing the I2circuit virtual-circuit-id in an NSR scenario. [PR1345949](#)

Resolved Issues: 17.3R2

Application Layer Gateways (ALGs)

- IPsec IKEv2 negotiation fails with IKE ALG enabled. [PR1300448](#)

EVPN

- The traffic might drop after receiving an updated ARP route packet from the peer Layer 3 gateway in an EVPN and VXLAN scenario. [PR1306024](#)
- Split horizon label is not allocated when the ESI configuration switches from **single-active** to **all-active**. [PR1307056](#)
- Core link flap might result in an inconsistent global MAC count. [PR1328956](#)

Forwarding and Sampling

- Some account files might be missed in case the remote archive sites are unreachable. [PR1300764](#)
- There is a memory leak on mib2d when polling firewall MIBs. [PR1302553](#)
- ACCT_FORK_LIMIT_EXCEEDED log level is ERROR even when the backup-on-failure feature is enabled for accounting files. [PR1306846](#)
- The second archive site in the accounting-file configuration is not used when the first one uses SFTP and is not reachable. [PR1311749](#)
- Accounting files with no records might be unexpectedly uploaded to the archive site. [PR1313895](#)
- The commit might fail when the **nexthop-learning** configuration statement is enabled for J-Flow v9. [PR1316349](#)
- Some firewall filter counters might not be created in SNMP. [PR1335828](#)

General Routing

- On MX Series platforms, the configuration of enhanced-IP and enhanced-Ethernet network mode is not compatible with MS-DPC card. Hence, the MS-DPC might not work correctly. [PR1035484](#)
- Ksyncd might crash because of the transient replication errors between Routing Engines. [PR1161487](#)
- Stale VBF states occur without sdb sessions. [PR1204369](#)
- The MS-MPC card might crash when OSPFv3 IPv6 traffic goes through it. [PR1233459](#)
- The **multicast-replication** setting cannot be reflected in the redundancy environment after rebooting both Routing Engines. [PR1240524](#)
- Disabling and enabling the "family mpls" of the next-hop interface might cause the route to be in a dead state in a BGP and MPLS scenario with a route of indirect next hop type. [PR1242589](#)
- The **validation-state:unverified** routing entry might not be shown with proper location when users run **show route**. [PR1254675](#)

- The rpd might crash during the next-hop change if unicast reverse-path- forwarding (uRPF) is used. [PR1258472](#)
- Status LED for the ge-0/0/0 interface does not glow. [PR1259112](#)
- PCC controlled LSP metric is not getting updated on the controller, PCE delegated LSPs do not come up. [PR1265864](#)
- MPC might report a parity error with the **fast-lookup-filter** configuration statement. [PR1266879](#)
- On MX Series routers, **show chassis led** command should not be displayed in possible completions of the **show chassis** command. [PR1268848](#)
- A low memory condition putting the service PIC into the red zone on the MS-MIC or MS-MPC card might cause the SIP ALG to generate a core file. [PR1268891](#)
- On MX Series platforms, if a large number of routes are processed, then the Packet Forwarding Engine of the MS-MPC might crash. [PR1277264](#)
- I2C BUS stuck causes SFP+ thread hogging and restarting of MPC. [PR1277467](#)
- The bbe-smgd process might generate a core file in certain cases when using iflsets in universal call admission control policy mode. [PR1278543](#)
- The chassis network services does not get set as "Enhanced-IP". [PR1279339](#)
- After an MS-MPC PIC goes offline or online or gets bounced (because of an AMS configuration change), sometimes the PIC can take approximately 400 seconds to come up. [PR1280336](#)
- Syslog messages **CM_FPC: Error requesting SET BOOLEAN, illegal setting 132,111** are seen after a unified ISSU from Junos OS Release 16.2R2 to Junos OS Release 17.1R2. [PR1280878](#)
- BIOS firmware upgrade or downgrade support is not available with Junos OS Release 17.3R1. [PR1281050](#)
- The **ingress service-accounting-deferred** command is not providing the correct IP traffic statistics for L2BSA subscribers. [PR1281201](#)
- Subscribers might not be able to connect to MX Series BNG in certain scenarios. [PR1281896](#)
- The kernel might crash in a rare corner case. [PR1282573](#)
- Layer 2 circuit will flap repeatedly, after the link up between PE and CE devices in "asynchronous-notification" and a specific CE device environment. [PR1282875](#)
- Error messages such as **IFRT: 'IFL**, **IFRT: 'Aggregate interface** and **IFRT: 'IFD** are seen when there is a change in configuration. [PR1282938](#)
- On MX Series routers, the CLI command **show interfaces** does not display the reason for bringing down the interfaces when the Packet Forwarding Engine is disabled. [PR1283323](#)
- The log message **VTAG not found in uflow** might be seen when a PPPoE subscriber logs on to a static VLAN logical interface. [PR1284966](#)
- LC, PFH, and Packet Forwarding Engine interface is not coming up on RE1. [PR1285606](#)

- With CoS-based forwarding, when the primary path of one of the next-hop LSPs flaps, traffic carried by the other next-hop LSP could get load-balanced across the primary and secondary paths. [PR1285979](#)
- Internal latency increases overtime for Packet Forwarding Engine sensors with streaming telemetry. [PR1286286](#)
- The missing statement “Shared bandwidth policer not supported for interface ge-x/x/x” is seen, during a failed commit in Junos OS Release 16.1R3. [PR1286330](#)
- Unified ISSU is not supported in Junos OS Release 15.1 or later releases, because the source release includes one or more BBE features such as logical interface (IFL) options, CoS fragmentation map, MLPPP, advisory options, advanced services, and multicast distribution. [PR1286507](#)
- DDoS culprit flows are not reported by CLI or logs in a single Packet Forwarding Engine MX Series router. [PR1286521](#)
- Framed routes might get stuck in the KRT queue. [PR1286849](#)
- The A10NSP interface does not get attached to the Layer 2 routing instance after renaming the routing instance. [PR1287070](#)
- SNMP query for 'IF-MIB::ifOutQLen' reports the wrong type. It should be Gauge32 or Unsigned32 for a dynamic VLAN DEMUX0 interface. [PR1287852](#)
- During unified ISSU (FRU upgrade) micro BFD flap is observed. [PR1288433](#)
- Performance issues can be seen when nontranslated traffic is introduced to a service set using a large number of NAT terms. [PR1288510](#)
- After GRES, smid was declared thrashing and was not restarted after a fatal SDB error. [PR1288871](#)
- Kernel "rtdat" memory leak is found on an MX Series Virtual Chassis with the configuration statement heartbeat enabled. [PR1289363](#)
- The FPC memory leak might happen in a BBE subscriber environment. [PR1289365](#)
- The interfaces might go down state after performing GRES. [PR1289493](#)
- The **request system zeroize** command deletes the **/var/db/scripts** directory which does not get re-created until the next USB or Netboot recovery. [PR1289692](#)
- The output **jnxContainersType** is not displayed for PIC and MIC as correctly as it is displayed on other Juniper Networks platforms. [PR1289778](#)
- If any of the vmhost applications are not running, then the alarm string will have "Application" name embedded in it. [PR1290150](#)
- The NAT-T and DPD functionality do not work for aggressive mode. [PR1290689](#)
- Incorrect temperature is displayed for MPCP5 and MPC7 in **show chassis fpc** output. [PR1290771](#)
- Memory leak occurs in the bbe-smgd daemon on subscriber logout for subscribers who have joined any multicast group. [PR1290918](#)
- LSP traffic might silently drop and get discarded after a link goes down in the bypass path. [PR1291036](#)

- The routing protocol process might generate a core file when restarting the process using a CLI command. [PR1291110](#)
- The switch might incorrectly learn its own IRB MAC address. [PR1291184](#)
- Device might lead to the DB prompt `db@jsr_jsm_send_ka_after_merge,send_proto_keealive`. This is observed on master Routing Engine. [PR1291247](#)
- The **Rescue configuration is not set** minor alarm getting set for MX10003. [PR1291525](#)
- l2tp incoming-call-connected messages retransmit fast and declare that the tunnel is down. [PR1291557](#)
- An error in `vbf_filter_add_orphan_check` might be seen when the subscribers use filter log out or log in. [PR1292582](#)
- An error message might be seen while bringing up the subscriber in a subscriber management environment. [PR1293057](#)
- **DDR3 TEMP ALARM** messages are logged in the chassisd log. [PR1293543](#)
- The `show extensible-subscriber-services sessions` command displays an incorrect timestamp after a unified ISSU. [PR1293800](#)
- On MPC6E linecard inline sampling, the flow export rate remains lower than the configured export rate. [PR1294296](#)
- Loss of DHCP and PPPoE subscribers is observed during unified ISSU from Junos OS Release 16.1-20170718_161_r4_s5.0 to Junos OS Release 16.1-20170718_161_r4_s5.0. [PR1294709](#)
- An rpd core file is generated after interface or BGP flapping. [PR1294957](#)
- The KRT queue might get stuck with the error of `RPD_KRT_Q_RETRIES: chain nexthop add: Unknown error: 0`. [PR1295756](#)
- The bbe-smgd process might generate a core file at `bbe_mcast_ifl_vbf_encoder` on service activation or deactivation along with smg-service daemon restart. [PR1295938](#)
- The service profile's CoS might be overridden by the client profile's CoS when second family DHCP sessions are added in a dual-stack subscriber scenario. [PR1296002](#)
- TACACS remote user is unable to run JET applications because of a bad stored heap. [PR1296237](#)
- The mspmand process might crash when using TDF gateway services on MS-MPC and MS-MIC. [PR1296422](#)
- The jdhcpd might crash when using 'dhcp-security' related command in enhanced subscriber management. [PR1296461](#)
- LLDP sensor on telemetry uses a lot of bandwidth. [PR1296869](#)
- The kernel might crash continuously when a lot of terms are configured for firewall filters. [PR1296884](#)
- In ECMP fast reroute scenario, traffic might get silently dropped and discarded because next hop is in "hold" state. [PR1297251](#)

- The bbe-smgd memory leak occur in multicast through dax/ddl. [PR1297454](#)
- When a service multicast profile uses variables for group policy or optical internetworking forum (OIF) or SSM-MAP-POLICY and if nonexistent policy names are sent down from the external system during service activation, core files are generated. [PR1297612](#)
- The routing protocol process crashes and generates a core file. [PR1298587](#)
- The commit error [**First_Net**] is thrown when trying to commit a configuration with applied groups. [PR1298649](#)
- The bbe-smgd process might crash when traceoption is enabled because of an invalid username character. [PR1298667](#)
- The bbe-smgd core files are constantly generated while running ESSM and PPPoE stress test with concurrent GRES. [PR1298742](#)
- MX Series BNG does not respond to PADI after GRES on some ports and VLANs. [PR1298890](#)
- When the subscriber limit feature is configured, any new login request after the maximum number of subscribers is denied. [PR1298924](#)
- The "asynchronous notification" feature cannot be implemented properly in a circuit that has MIC-3D-20GE-SFP-E and Tri Rate Copper SFP(740-013111). [PR1299574](#)
- Flat accounting files are not generated according to the configured timers. [PR1299597](#)
- Subscriber database is stuck in "not ready" state after GRES. [PR1299940](#)
- After IS-IS TE routes and BGP routes attribute change, traffic loss might be seen because BGP routes point to some stale labels. [PR1300425](#)
- The error **error: the SDN-Telemetry subsystem is not responding to management requests** is seen on issuing the CLI command **show agent sensors** if traceoptions are enabled for service analytics. [PR1300829](#)
- ICMP and ICMPv6 error messages might be discarded while forwarding through an AMS interface. [PR1301188](#)
- Configured sub-interface might not be created correctly after commit. [PR1301823](#)
- Continuous interface flapping might lead to unwanted MIC reset. [PR1302246](#)
- The rpd might crash when toggling **vrf-propagate-ttl** and **no-vrf-propagate-ttl** configuration statements. [PR1302504](#)
- Chassisd.core-tarball.0.tgz is found during unified ISSU aborted in FRU upgrade phase. [PR1303086](#)
- Incorrect MTU might be seen on PPP interfaces, when PPP MTU is not defined in the dynamic profile. [PR1303175](#)
- The list of available routing instances is no longer provided for output of the **show subscribers routing-instance** command. [PR1303199](#)
- The inline-ka PPP echo requests are not generated for aggregated Ethernet interfaces. [PR1303249](#)

- Blocking PPPoE or DHCP to initiate VLAN auto-sensing, if VLAN-OOB connected is in pending state. [PR1303338](#)
- Fan speed changes frequently on MX Series Virtual Chassis. [PR1303459](#)
- MX Series router with MIB polling returns a value that has "sdg". Polling result should include svc generic value. [PR1303848](#)
- Truncated output is shown for the **show pppoe lockout** CLI command. [PR1304016](#)
- Effective rate of E3 in framed mode is limited to 30 Mbps on certain channelized MICs. [PR1304344](#)
- RPF-check strict causes traffic drop in next-generation subscriber management release. [PR1304696](#)
- Commit fails with error **ffp_intf_ifd_hier_tagging_config_verify: Modified IFD "si-1/1/0" is in use by BBE subscriber, active L2TP LNS client**. [PR1304951](#)
- Inline J-Flow vMX: OIF field of VPLS data records sometimes report SNMP index value of LSI interface instead of egress physical interface. [PR1305411](#)
- MX Series router sends immediate-interim for the services pushed by SRC. [PR1305425](#)
- The routing protocol process (rpd) crashes on loading EVPN configurations. [PR1305440](#)
- JET **daemonize** application restarts even on normal exit. [PR1305615](#)
- L2BSA subscriber connection attempts failed with VLAN profile-request-error. [PR1305962](#)
- L2BSA subscribers came up, while no new ANCP session got established during the RADIUS disaster backup procedure. [PR1306872](#)
- Smihelperd generates core files when SNMP is polling for JUNIPER-SUBSCRIBER-MIB::jnxSubscriberGeneral.7.0. [PR1306966](#)
- IPsec key management process (kmd) stops key exchange process after sending out **UI_DBASE_OPEN_FAILED Too many open files** error message. [PR1308380](#)
- License is lost during Routing Engine switchover in scale-subscriber scenario. [PR1308620](#)
- CoS applied to a subscriber demux logical interface (IFL) is not working. [PR1308671](#)
- All the MICs on FPC, with PS interfaces configured, went offline during the restart of the FPC in another slot. [PR1308995](#)
- Error messages **%PFE-3: fpc0 vbf_var_iflset_add:633: vbf container 11 not found in the msg for ifl .demux.6514** are often seen after MPC restart. [PR1309013](#)
- Incorrect values are found in the event-timestamp of RADIUS accounting-stop packets for L2BSA subscribers. [PR1309212](#)
- On MX2020 and MX2010, after smooth SFB to SFB2 upgrade, if one plane is restarted, link training fails between that plane and the MPC6 cards. [PR1309309](#)
- First access-request fails for L2BSA subscribers when changing the MTU of LACP aggregated Ethernet A10NSP interface. [PR1309599](#)

- DHCP client gets stuck in selecting state while verifying untagged DHCP subscribers after modifying router configuration. [PR1309730](#)
- DT_BNG : 9000 out of 10000 terminated subscribers go down during the unified ISSU from Junos OS Release 16.1 through Junos OS Release 17.3. [PR1309983](#)
- The bbe-smgd process memory leak might be seen after deleting or adding the address pool in next-generation subscriber management release. [PR1310038](#)
- The MS-MIC and MS-MPC memory utilization might stay at high level in the subscriber management scenario. [PR1310064](#)
- **SPD_CONN_OPEN_FAILURE** and **SPC_CONN_FAILURE** log messages are seen in the logs for SI interfaces when running SNMP walk on service PIC NAT OIDs. [PR1310081](#)
- **krt_junos_sanity_check_ctrl_resp: rtsock** request finally succeeded after error 16 syslog message in Junos OS Release 17.1R1.8. [PR1310678](#)
- Local IPv6 interface from NDRA prefix is not removed from service interface, while subscriber dual-stack session is removed. [PR1310752](#)
- After bsys reboot sometimes rpd is unresponsive on one or more GNFs. [PR1310765](#)
- Bad stored heap: heap-ptr=0x0 data-ptr=0x1481cbf8. [PR1311482](#)
- The FPC memory might be exhausted with SHEAF leak messages seen in the syslog. [PR1311949](#)
- Counter at PPPoE session logical interface increments incorrectly, causing the accounting packet to contain incorrect acct-input-packets value and incorrect acct-input-octets value. [PR1312998](#)
- The CLI command **show version detail | no-more** hangs for more than 120 seconds in the master Routing Engine and more than 60 seconds in the backup Routing Engine. [PR1314242](#)
- The smgd process generates a core file with reference to bbe_cos_ifl_publish() bbe_cos_if.c:6543. [PR1314651](#)
- The rpd might crash in MoFRR scenario. [PR1314711](#)
- The RIB and FIB might get out of synchronization because the KRT asynchronous queue might get stuck. [PR1315212](#)
- The CLI command **show version detail** gives severity error log **main: name: SRD ret: 0**. [PR1315436](#)
- Transit traffic over GRE tunnel might hit the CPU and trigger a DDoS violation on the L3 next hop. [PR1315773](#)
- The **show auto-configuration out-of-band** CLI command used with a different configuration statement shows the same output. [PR1316661](#)
- Demux interface sends neighbor solicitation with source link-address of all zeros 00:00:00:00:00:00 MAC. [PR1316767](#)
- The rpd might crash when the link flaps on an adjacent router. [PR1318476](#)
- MS-MPC and MS-MIC might crash after a new IPsec tunnel is added. [PR1318932](#)

- MX Series routers sends the IPv6 router advertisements and the DHCPv6 advertisements before sending IPCPv6 ACK from CPE. [PR1321064](#)
- In commit fast-synchronize mode, the commit operation might get stuck after the **commit check** is performed. [PR1322431](#)
- An incorrect output is observed while verifying the command **show subscribers client-type vlan subscriber-state active logical-system default routing-instance default**. [PR1322907](#)
- Subscribers might fail to login after the interface is deactivated or activated. [PR1324446](#)
- Approximately three percent of Packet Forwarding Engine forwarding capacity might be seen on XM-chip when its temperature is higher than 67 degrees Celsius. [PR1325271](#)
- Minor alarm **LCM Peer Connection un-stable** on the MX150. [PR1328119](#)
- When using **show subscribers** and FPC number has two digits, the interface and IPv6 address get connected together for DHCPv6 PD. [PR1334904](#)

High Availability and Resiliency

- Insufficient available space on hard disk lead by the crashinfo files is generated by ksyncd when GRES is configured in large-scale configuration scenario. [PR1332791](#)

Infrastructure

- The "Last flapped" time stamp is not getting updated for fxp0 interface as per the expectation. [PR1244502](#)
- The **show system users** CLI command output displays more users than are actually using the router. [PR1247546](#)
- The MX Series router might fail to upgrade Junos OS Release 14.2R6 to Junos OS Release 16.1R4. [PR1298749](#)
- The syscalltrace.sh might create a huge output file, which could cause the router to run out of storage space. [PR1306986](#)

Interfaces and Chassis

- The output value is incorrect when querying the optical power of OTN interfaces on the router. [PR1216153](#)
- [SIRT] MX Series Packet Forwarding Engine and MX Series MPC7E, MPC8E, and MPC9E Packet Forwarding Engine crash when fetching interface statistics with extended-statistics enabled (CVE-2017-10611). [PR1247026](#)
- At a high logical interface scale, an ifinfo process (daemon) generates a core file on executing the command **show interfaces**. [PR1254189](#)
- Monitor interface on aggregated Ethernet logical interfaces displays incorrect bps value compared to **show interface** output. [PR1283831](#)
- The family inet shows as not configured after adding or deleting the loopback address. [PR1294267](#)

- A VRRP track interface-down does not trigger a mastership election immediately. [PR1294417](#)
- IRB interface is showing incorrect bandwidth value. [PR1302202](#)
- AFEB might not come up when LFM is deactivated. [PR1306707](#)
- After executing **request system reboot both** CLI command, the Juniper PPP daemon might become unresponsive. [PR1310909](#)
- The PPPoE subscriber might not log in correctly after authentication failure. [PR1311113](#)
- MX Series Virtual Chassis unified ISSU emits benign error message if unsupported FRUs are present. [PR1316374](#)
- IPv6 Framed Interface Id field is not showing correctly in **show subscribers extensive** output. [PR1321392](#)
- The interface might not work properly after FPC restarts. [PR1329896](#)

Layer 2 Features

- A misconfiguration adds an aggregated Ethernet interface bundle, and its member links to a VPLS instance might cause 100 percent routing protocol process (rpd) utilization. [PR1280979](#)
- On MX Series routers with MPCs or MICs based platforms, packets received on the IRB interface in virtual private LAN services (VPLS) get double tagged. [PR1295991](#)

Layer 2 Ethernet Services

- DHCPV6 client bound to IA_PD prefix on reception of DHCPV6 request for IA_NA, MX Series deletes the existing binding. [PR1286359](#)
- ARP requests are not generated for IRB configured in VPLS over GRE tunnel. [PR1295519](#)
- In a PPPoE and DHCP dual-stack subscriber scenario with an incorrect DHCP configuration, MX Series router might eventually stop logging in PPPoE and DHCP clients. [PR1298976](#)
- Multiple jdncpd core files are observed in jdncpd_update_groups at `../../../../src/junos/usr/sbin/jdncpd/jdncpd_config.c:2290`. [PR1311569](#)

MPLS

- RSVP p2mp sub-LSPs having more than one sub-LSP in down state might not get re-optimized after transit path goes down. [PR1174679](#)
- The rpd might crash when moving static LSP from one routing instance to another. [PR1238698](#)
- The created time value in **show mpls lsp extensive** might drift by a second when the **show** command is issued multiple times. [PR1274612](#)
- MPLS layer 2 circuit ping packet is incorrectly parsed by the output loopback filter. [PR1288829](#)
- Received MTU might not get updated in RSVP MTU signaling. [PR1291533](#)
- Stale RSVP LSP entry occurs after NSR switchover and session is not refreshed. [PR1292526](#)
- The rpd might crash if MPLS LSP path change occurs. [PR1295817](#)

- When using IS-IS traffic engineering (TED), if an LSP's state changed, routing protocol process might lose track of memory. [PR1303239](#)
- BGP multipath might not work when interface flaps. [PR1305228](#)
- Feature "explicit-null" might block host-bound traffic incoming from LSP. [PR1305523](#)
- The rdp process might crash during interface-down events when UHP-based LSPs are configured. [PR1309397](#)

Network Management and Monitoring

- Mib2d-related syslog messages **MIB2D_RTSLIB_READ_FAILURE: rtllib_iflm_snmp_pointchange** are seen during remove and restore configurations. [PR1279488](#)
- The mib2d process might crash when polling the OID ifStackStatus.0 after a logical interface of lo0 is deleted. [PR1286351](#)
- The **show arp no-resolve interface X** command output for nonexistent interface X is showing all unrelated static ARP entries. [PR1299619](#)
- After SNMP configuration activation, the snmpd process started to consume more CPU time. [PR1300016](#)
- The syslog duplicate entries of hostname and timestamp are breaking the standard logging format. [PR1304160](#)

Platform and Infrastructure

- Traffic drop might occur under a large-scale firewall filter configuration. [PR1093275](#)
- The "forwarding-class-accounting enhanced" feature is not supported in combination with "forwarding-options hyper-mode". Using both features together results in traffic getting silently dropped and discarded. [PR1198021](#)
- The dexp process might crash after committing **set system commit delta-export**. [PR1284788](#)
- Generate-event time-interval usage now triggers the event only on the actual expiry of time interval. [PR1286803](#)
- Incorrect load-balance on ae interface might occur if traffic transits from MS-DPC to MPC card in enhanced-IP mode. [PR1287086](#)
- Packet Forwarding Engine heap memory leak was found in three routers with PPPoE subscribers. [PR1287870](#)
- While adding a new package to the router, you might see the following message: **mgd: error: Could not open library: /usr/lib/render/libvccpd-render.tlv**. [PR1289158](#)
- The syslog error **not a proper library: /usr/lib/render/libdcd-render.so: Cannot open "/usr/lib/render/libdcd-render.so** appears when any non-superuser/non-root user tries to log in to the router.. [PR1289974](#)
- Dynamic MAC learning might fail on GRE tunnel interface. [PR1291015](#)

- The scale-subscriber license might leak on the backup Routing Engine during bulk subscriber logout. [PR1294104](#)
- The management daemon might crash and generate a core file after GRES in a subscriber environment. [PR1298205](#)
- **RMOPD_HW_TIMESTAMP_INVALID** is reported two to four times a day, which raises an alarm when polled through **jnxRpmResSumPercentLost** MIB. [PR1300049](#)
- On MX Series platforms with firewall filter configuration, the MPC might reset while loading the configuration. [PR1300990](#)
- All traffic can be tail-/RED-dropped on some interfaces when **chassis fpc max-queues** is configured. [PR1301717](#)
- Classifier does not get applied on the ae member links on DPC (I-chip) based platforms with CoS configured. [PR1301723](#)
- MX Series FPC wedges when creating more than 4000 logical-tunnel interfaces per Packet Forwarding Engine. [PR1302075](#)
- The CLI command **mk destroy-all** is displaying the error **Could not find jnx.wrlsb.mk**. [PR1302974](#)
- The interface-mac-limit might fail for ae interface. [PR1303293](#)
- The **TWAMP Request-TW-Session** message Type-P descriptor format is not RFC-compliant. [PR1305752](#)
- jlaunchd: System reaching processes ceiling <low or high or critical> watermark because of auditd. [PR1305964](#)
- On MX Series routers with MPCs or MICs, the resource monitor (RSMON) thread might get stuck in a loop, consuming 100 percent of FPC CPU. [PR1305994](#)
- The **show system resource-monitor fpc slot <>** command reported memory free percentages that were not accurate. [PR1287592](#)
- The source MACs might leak (or not learn) between different VPLS instances at the receiving end VPLS PE devices. [PR1306293](#)
- This PR addresses the ICMP error messages in Packet Forwarding Engine and is forwarded to the correct pic in the AMS bundle. [PR1313668](#)
- Multicast traffic is not forwarded on the newly added p2mp branch and receiver. [PR1317542](#)
- Multicast traffic might get duplicated when MoFRR is configured. [PR1318129](#)
- Errors might be observed when the **fabric-header-crc-enable** statement is enabled. [PR1320874](#)
- RPM probes delegated to MS-MIC get stuck when any change is made to the BGP group stanza. [PR1322097](#)

Routing Policy and Firewall Filters

- The rpd might crash when **vrf-target auto** is configured under routing-instance. [PR1301721](#)

Routing Protocols

- No multicast forwarding in ASM mode occurs after unified ISSU. [PR1146621](#)
- MPLS over UDP tunnel creation fails in absence of a routing instance table. [PR1270955](#)
- The rpd might crash after deactivating or activating BGP. [PR1272202](#)
- A few bfd sessions flap while coming up after FPC reboots. [PR1274941](#)
- BGP updates might not be advertised to peers completely under certain conditions. [PR1282531](#)
- Some BGP-related traceoptions flag settings might not take effect until the BGP sessions are flapped. [PR1285890](#)
- With BGP traceoption enabled, executing the rollback and load merge commands for the configuration might cause rpd to crash. [PR1288558](#)
- BGP-RR sends full route updates to its RR-Clients when any family MPLS interface bounces because of any fiber cut or manual events causing high CPU spike. [PR1291079](#)
- BGP Monitoring Protocol (BMP) might send malformed route monitoring messages. [PR1292848](#)
- The rpd might crash if BGP flap occurs. [PR1295062](#)
- The backup Routing Engine scheduler slips when the import policy is configured improperly. [PR1295712](#)
- Unified ISSU might take more time to complete and the MPC card might go offline during unified ISSU reboot. [PR1298259](#)
- The rpd process might crash because of the AS PATH check error that occurs when RIB groups are added first and later the routing instances are added. [PR1298262](#)
- Inline-BFD on IRB will be broken after GRES or NSR switchover and the subsequent anchor FPC goes offline. [PR1298369](#)
- BGP might send an incorrect AS path when an alias is enabled and multiple peers are under the BGP group. [PR1300333](#)
- The rpd process might crash and generate a core file while deleting a multipath route. [PR1302395](#)
- The mcsnoopd process generates a core file during task cleanup. [PR1305239](#)
- Junos OS Release 16.2 and later releases might give the following error: **Request failed: OID not increasing: ospfIfIpAddress.0.0.0.0.0** . [PR1307753](#)
- The route's next-hop resolution might fail if the static route is configured with **qualified-next-hop** and **resolve** options over a numbered interface. [PR1308800](#)
- BGP labeled-unicast protection might break multicast RPF. [PR1310036](#)
- The rpd process generates a core file in **bgp_rt_send_message** at `../../../../src/junos/usr/sbin/rpd/bgp/bgp_io.c:1460`. [PR1310751](#)

- The BGP session might flap when the connection between the master Routing Engine and the backup Routing Engine keeps flapping with NSR configured. [PR1311224](#)
- The rpd might crash when the neighbor IS-ISv6 router is restarted, causing route churn. [PR1312325](#)
- IS-IS SPF gets triggered by LSP updates containing changes in the reservable bandwidth in traffic engineering extensions. [PR1313147](#)
- BGP prefixes with three levels of recursion for resolution will get stuck with a stale next hop at the first level after a link-down event. [PR1314882](#)
- On a chassis with BMP configured, the rpd might crash when the rpd process is gracefully terminated. [PR1315798](#)
- BGP-LU update oscillation occurs with BGP-PIC. [PR1318093](#)
- Need to remove the syslog message that got added to code unintentionally. [PR1318458](#)

Services Applications

- TLVs in ICRQ for **actual-rate-downstream** and **actual-data-rate-upstream** do not reflect PPPoE-IA value. [PR1286583](#)
- Mspmand core file "@_arena_mALLOc" is seen in backup SDG's MS70. [PR1291664](#)
- L2TP subscribers are down after a GRES while verifying the framed IPv6 route support for L2TP network server (LNS) at a higher scale with a maximum number of Framed-IPv6-Route. [PR1293783](#)
- The jl2tpd process might crash shortly after a GRES switchover. [PR1295248](#)
- L2TP subscribers might get stuck in terminating state during login. [PR1298175](#)
- The "jl2tpd_era_lns" log files are continuously generated even when L2TP is not configured. [PR1302270](#)
- LTS clients experience packet drop in large packets because of fragmentation in LTS. [PR1312691](#)
- AVP 145 is not present in IRQ when ANCP DSL-type = 0. [PR1313093](#)
- IPCP active mode is not enabled for MLPPP on LNS. [PR1319580](#)

Software Installation and Upgrade

- Junos Selective Update (JSU) package is not activated after a reboot. [PR1298935](#)

Subscriber Access Management

- Service interim for DHCP subscriber is not working in JSRC scenario. [PR1303553](#)
- The output of the **show network-access aaa accounting** command might display additional entries. [PR1304594](#)
- Incorrect Acct-Delay-Time in RADIUS Accounting-On message after rebooting the MX Series BNG. [PR1308966](#)
- When the subscriber is removed manually or through a script, memory leak might be seen. [PR1312517](#)

- The delegated prefix from RADIUS is parsed incorrectly when the length is less than 20 bytes. [PR1315557](#)
- Unified ISSU is not allowed when the account is suspended. [PR1320038](#)
- Authd considers RADIUS attribute Framed-IPv6-Prefix = ::/64 or Delegated-IPv6-Prefix = ::/56 as valid parameters. [PR1325576](#)

VPNs

- Next-generation MVPN SG entry and MVPN route persist after data stop. [PR1236733](#)
- Next-generation MVPN IPv6 RP bootstrap type 3 S-PMSI AD route prefix ff02::d persists after BSR data stop. [PR1269234](#)
- Layer 2 circuits stitched through It peer interfaces might get stuck in local site signal down (LD) status. [PR1305873](#)

Resolved Issues: 17.3R1

Class of Service (CoS)

- The Routing Engine level **scheduler-hierarchy** command misses a forwarding class when the "per-unit-scheduler" mode is configured. [PR1281523](#)

Forwarding and Sampling

- Unexpected messages might be seen in logs. [PR1270686](#)
- The sampled process stops collecting data on Routing Engine based sampling supported platforms. [PR1270723](#)
- The sampled process might crash if traceoptions are enabled. [PR1289530](#)

General Routing

- On MX240/480/960 platforms, due to I2C bus hardware issue, FPC might reboot and error message might appear. [PR1174001](#)
- In MX Series subscriber management environment, the rpd might crash in the backup Routing Engine after executing Routing Engine switch over. [PR1206804](#)
- On MX Series routers with MPC2E-3D-NG/MPC2E-3D-NG-Q/MPC3E-3D-NG/MPC3E-3D-NG-Q line card, if the FPC-MIC link failure happens, the bridge might keep sending register messages in an infinite loop, which would cause continuous PCI exceptions, the MPC might crash and traffic forwarding might be affected. This is a rare issue, it is hard to reproduce. [PR1231167](#)
- XM chip based line card (MPC3E/4E/5E/6E/2E-NG/3E-NG) might drop traffic under high temperature (67C or higher). [PR1244375](#)
- On MX2000 with MPC6E, EOAM LFM adjacency flaps when an unrelated MIC accommodated in the same MPC6E slot is brought online by configuring OAM pdu-interval 100 ms and pdu-threshold 3. [PR1253102](#)

- When unified ISSU is performed under scaled scenarios where the Packet Forwarding Engine next-hop memory uses more than 4 Million Dwords, PPE traps and traffic loss may be observed during the software-sync phase until the end of the hardware sync. [PR1267680](#)
- The mspmand log messages about memory zone level which should not be generated are generated. It will occur every 49.7 days and will recover by itself. This is a display issue and will not affect the traffic. [PR1273901](#)
- The CLI commands fails for the following commands: **show subscribers detail**, **show subscribers extensive**, **show subscribers count client-type <>**, and other commands. The failure occurs because the subscriber-management database is unavailable. [PR1274464](#)
- Link stays down after a flap on MPC next generation cards with QSFP+-40G direct attach copper (DAC). [PR1275446](#)
- VT interface flaps during unrelated commit operations if MTU is configured on it. [PR1277600](#)
- vlan-oob subscriber session fails in autoconfd due to physical interface down even if the interface is up. [PR1279612](#)
- **MIC Error code: 0x1b0001** alarm was not clear even after the voltage was returned to normal. [PR1280558](#)
- In a subscriber management environment, if authenticated subscriber dynamic VLAN receives idle timeout from the Radius server, due to a rare timing issue such dynamic VLAN interface can be removed immediately after it was successfully created. [PR1280990](#)
- Establishment of IPsec SAs for link type tunnels might fail under certain conditions in case of scaled IPsec link type service set configuration. In such cases the inside IFL corresponding to service set would remain down. This can be resolved by restarting ipsec-key-management daemon by issuing the following command -----8< -----8< ----- restart ipsec-key-management -----8< -----8< ----- Additionally sometimes the traffic may be affected after restarting IPsec management daemon. Clearing IPsec SAs corresponding to such service set would resolve this issue. This can be achieved by running the following commands -----8< -----8< ----- clear services ipsec-vpn ipsec security association <service-set> -----8< -----8< ----- [PR1281223](#) [PR1281223](#)
- DHCP/PPPoE subscribers fail to bind after FPC restart and smgd restart with BBE_RTsock_GET_RTsock_IFL_FAIL_TERMINATED counter going up. [PR1281930](#)
- Inline-JFlow unrelated configuration changes related to a routing-instance results in invalid/incomplete JFlow data packets. Commit-full resumes proper functionality. [PR1282580](#)
- Error messages related to "IFRT: 'IFL'", "IFRT: 'Aggregate interface'" and "IFRT: 'IFD'" seen on config change [PR1282938](#)
- VBF flows are not programmed correctly on ae interfaces resulting in 50% traffic loss. [PR1282999](#)
- OAM fails to come up when GRE tunnel source and family inet address are the same. [PR1283646](#)
- PPTP session could not be established on MSMPC when it is bothstateful-firewall and NAT enabled, and the address could not be translated. [PR1285207](#)

- Possible High CPU on MPC4E when interfaces have been disabled by administrator. [PR1285673](#)
- The J-Flow data template sequence number is zero for MPLS flows. [PR1285975](#)
- Process routing protocol daemon might crash while logging in or logging out with multicast service enabled and performing a GRES switchover. [PR1286653](#)
- L2TP tunnel switch functionality is not working on Junos OS Release 16.1R4 if rewrite-rule configuration is applied to the dynamic profile. [PR1287788](#)
- services-oids-ev-policy.slax & services-oids.slax files built in Junos OS images are not using latest versions. [PR1287894](#)
- After offlining and onlining fabric planes, a few planes are stuck in the offline state in the MX480 router. [PR1287973](#)
- Backup bbe-smgd.core with distributed IGMP configuration. [PR1288465](#)
- If any of the vmhost application is not running then the alarm string will have "Application" name embedded in it. [PR1290150](#)
- BBE-SMGD generates a core file following a stress test in bbe_iff_add_ifa. [PR1291969](#)
- CPCDD might generate core files while using Routing Engine-based http-redirect. [PR1293553](#)
- Not able to edit dynamic profiles after scaling up to 400 dynamic profiles. [PR1295446](#)
- bbe-smgd core at bbe_mcast_ifl_vbf_encoder on service activation or deactivation along with smg-service restarts. [PR1295938](#)

Interfaces and Chassis

- L2TP sessions are not coming up on some of si interfaces after an MPC restart followed by a Routing Engine switchover. [PR1290562](#)

Layer 2 Features

- All the XML duplications and unformatted output are addressed. For Example, histogram was just declared as a element inside pfkey container, with this change a new container is defined for histogram. [PR1271648](#)

Layer 2 Ethernet Services

- DHCP is not using the configured IRB MAC as the source MAC because DHCP is offering only unicast replies. [PR1272618](#)

MPLS

- NG-MVPN MLDP at the receivers' PE does not join P2MP LSP on changing the root PE route from IGP/LDP to LBGP. [PR1277911](#)

Network Management and Monitoring

- The command Esc-q does not work to toggle the console log/terminal log. [PR1269274](#)

- The MIB II process (mib2d) logs an "RLIMIT curr 1048576000 max 1048576000" message every time a commit is performed. [PR1286025](#)
- The mib2d process might crash when polling the OID ifStackStatus.0 after an IFL of lo0 is deleted. [PR1286351](#)

Platform and Infrastructure

- Traffic drop might occur under a large scale of firewall filter configuration. [PR1093275](#)
- FPC crashes with MAC accounting feature enabled. [PR1173530](#)
- FPC CPU spikes every 6 minutes on MX Series routers with MICs and MPCs chipsets due to micro code rebalance. [PR1207532](#)
- RPM loss percent values for "overall tests" through SNMP is incorrect. [PR1272566](#)
- The CLI command **request routing-engine login other-routing-engine** might require a password. [PR1283430](#)
- Transit traffic with DMAC starting with "02" will be punted to Routing Engine when mac-learn-enable is configured. [PR1285874](#)
- The source MAC learned over cross-PFE ae might bounce between ae member Packet Forwarding Engines for a long time and which might cause MLP-ADD storm. [PR1290516](#)
- RMOPD might get stuck in the sbwait state upon receiving a specific response from the HTTP agent. [PR1292151](#)

Routing Protocols

- Routing protocol daemon on the backup Routing Engine might restart unexpectedly upon the addition of a new L2VPN routing instance. [PR1233514](#)
- When the **advertise-from-main-vpn-tables** configuration statement is used under BGP and if RR functionality is added, a refresh message is not sent, and as a result, some routes are missed. [PR1254066](#)
- MPLSoUDP tunnel creation failure in the absence of a routing instance table. [PR1270955](#)
- After Routing Engine switchover (GRES+GR) default mdt failed to come up also seen with core facing interface flap. [PR1279459](#)
- Routing protocol daemon might crash due to a certain chain of events in the BGP-LU protection scenario. [PR1282672](#)
- The second multicast packet might be discarded on RP router. [PR1282848](#)
- Routing protocol daemon crashes while deactivating in a routing instance protocols pim static. [PR1284760](#)
- Routing protocol daemon might crash if dynamic RP goes down in ECMP topology when PIM join load balancing automatic is configured. [PR1288316](#)

Services Applications

- Business service fails to get deactivated post Routing Engine switchover. [PR1280074](#)
- Backup Routing Engine is going to the database prompt with a vmcore if the down ASI interface configuration is deleted. [PR1281882](#)
- Loss of all L2TP subscribers on an LAC router after smg-service restarts on the L2TP tunnel switch.. [PR1284260](#)
- The l2tpd process generates a core file with reference to 0x084166f5 in L2tpTunnel::createSucceeded (this=0xa04ae84, createFlags=...) at ../src/junos/usr.sbin/jl2tpd/l2tpTunnel.cc:1845. [PR1288029](#)
- Each subscriber session is getting its own L2TP tunnel without "Tunnel-Client-Endpoint" from radius. [PR1293927](#)

Subscriber Management and Services

- MX Series router could not filter some RADIUS attributes with the accounting-Off and accounting-On messages. [PR1279533](#)
- Authenticated subscriber dynamic VLAN interface might get disconnected immediately after a successful connection. [PR1280990](#)
- Authd core file is observed while terminating large number of subscribers. [PR1289215](#)

User Interface and Configuration

- The commitd process might generate a core file by certain configuration removal followed by a commit operation. [PR1267433](#)

VPNs

- Routing protocol daemon memory leak is observed in next-generation-MVPN environment. [PR1259579](#)

SEE ALSO

[New and Changed Features | 103](#)

[Changes in Behavior and Syntax | 135](#)

[Known Behavior | 145](#)

[Known Issues | 154](#)

[Documentation Updates | 214](#)

[Migration, Upgrade, and Downgrade Instructions | 215](#)

[Product Compatibility | 222](#)

Documentation Updates

IN THIS SECTION

- [Subscriber Management Access Network | 214](#)
- [Subscriber Management Provisioning Guide | 214](#)

This section lists the errata and changes in Junos OS Release 17.3R3 documentation for MX Series.

Subscriber Management Access Network

- The guide failed to include a feature that enables you to override the information that the LAC sends to the LNS in L2TP Calling Number AVP 22 when the LAC is configured to use the Calling-Station-ID format. You can configure the access profile to override that value for AVP 22 with any combination of the agent circuit identifier and the agent remote identifier received by the LAC in the PADR packet.

[See [Override the Calling-Station-ID Format for the Calling Number AVP](#)].

- The guide incorrectly stated that the **linked-pool-aggregation** statement is located at the **[edit access address-assignment pool pool-name]** hierarchy level. In fact, this statement is located at the **[edit access]** hierarchy level.

See [Configuring Address-Assignment Pool Linking](#).

Subscriber Management Provisioning Guide

- The *Broadband Subscriber Sessions User Guide* did not report that you can suspend AAA accounting, establish a baseline of accounting statistics, and resume accounting. This feature was introduced in Junos OS Release 15.1R4.

[See [Suspending AAA Accounting and Baselining Accounting Statistics Overview](#)].

- Starting in Junos OS Release 15.1, the *Broadband Subscriber Sessions User Guide* and the [CLI Explorer](#) incorrectly included information about the **show extensible-subscriber-services accounting** command. This command is not present in the CLI. Instead, you can use accounting profiles to collect statistics from the Packet Forwarding Engine for Extensible Subscriber Services Manager (ESSM) subscribers. [See [Flat-File Accounting Overview](#) for information about accounting for ESSM subscribers.]

SEE ALSO

New and Changed Features	103
Changes in Behavior and Syntax	135
Known Behavior	145
Known Issues	154
Resolved Issues	174
Migration, Upgrade, and Downgrade Instructions	215
Product Compatibility	222

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Basic Procedure for Upgrading to Release 17.3 | 216
- Procedure to Upgrade to FreeBSD 10.x based Junos OS | 216
- Procedure to Upgrade to FreeBSD 6.x based Junos OS | 218
- Upgrade and Downgrade Support Policy for Junos OS Releases | 220
- Upgrading a Router with Redundant Routing Engines | 220
- Downgrading from Release 17.3 | 221

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 with Junos OS Release 15.1, in some of the devices, FreeBSD 10.x is the underlying OS for Junos OS instead of FreeBSD 6.x. This feature includes a simplified package naming system that drops the domestic and world-wide naming convention. However, in some of the routers, FreeBSD 6.x remains the underlying OS for Junos OS. For more details about FreeBSD 10.x, see [Understanding Junos OS with Upgraded FreeBSD](#).

NOTE: In Junos OS Release 15.1, Junos OS (FreeBSD 10.x) is not available to customers in Belarus, Kazakhstan, and Russia. Customers in these countries need to use the existing Junos OS (FreeBSD 6.1).

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

Platform	FreeBSD 6.x-based Junos OS	FreeBSD 10.x-based Junos OS
MX80, MX104	YES	NO
MX240, MX480, MX960, MX2010, MX2020	NO	YES

Basic Procedure for Upgrading to Release 17.3

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 [Junos OS Administration Library](#).

For more information about the installation process, see [Installation and Upgrade Guide](#) and [Upgrading Junos OS with Upgraded FreeBSD](#).

Procedure to Upgrade to FreeBSD 10.x based Junos OS

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

To download and install FreeBSD 10.x based Junos OS:

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 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.

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-32-17.3R3.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-64-17.3R3.9-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**

Do not use the **validate** option while upgrading from Junos OS (FreeBSD 6.x) to Junos OS (FreeBSD 10.x). This is because programs in the **junos-upgrade-x** package are built based on FreeBSD 10.x, and Junos OS (FreeBSD 6.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 VM Host Installation topic in the [Installation and Upgrade Guide](#).

NOTE: After you install a Junos OS Release 17.3 **jinstall** package, you cannot return to the previously installed Junos OS (FreeBSD 6.1) 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: MX80, and 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://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 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.

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

```
user@host> request system software add validate reboot
source/jinstall-17.3R3.9-domestic-signed.tgz
```

- All other customers, use the following command:

```
user@host> request system software add validate reboot source/jinstall-17.3R3.9-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**

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 17.3 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

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 16.2, 17.1 and 17.2 are EEOL releases. You can upgrade from Junos OS Release 16.2 to Release 17.1 or even from Junos OS Release 16.2 to Release 17.2. However, you cannot upgrade directly from a non-EEOL 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://support.juniper.net/support/eol/software/junos/>.

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 17.3

To downgrade from Release 17.3 to another supported release, follow the procedure for upgrading, but replace the 17.3 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](#).

SEE ALSO

New and Changed Features 103
Changes in Behavior and Syntax 135
Known Behavior 145
Known Issues 154
Resolved Issues 174
Documentation Updates 214
Product Compatibility 222

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 222](#)

Hardware Compatibility

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

To determine the features supported on MX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at: <https://pathfinder.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

New and Changed Features 103
Changes in Behavior and Syntax 135
Known Behavior 145
Known Issues 154
Resolved Issues 174
Documentation Updates 214
Migration, Upgrade, and Downgrade Instructions 215

Junos OS Release Notes for NFX Series

IN THIS SECTION

- New and Changed Features | 223
- Changes in Behavior and Syntax | 224
- Known Behavior | 225
- Known Issues | 225
- Resolved Issues | 226
- Documentation Updates | 226
- Migration, Upgrade, and Downgrade Instructions | 227
- Product Compatibility | 228

These release notes accompany Junos OS Release 17.3R3 for the NFX 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.

New and Changed Features

IN THIS SECTION

- Release 17.3R3 New and Changed Features | 224
- Release 17.3R2 New and Changed Features | 224
- Release 17.3R1 New and Changed Features | 224

This section describes the new features and enhancements to existing features in the Junos OS main release and the maintenance releases for NFX Series.

Release 17.3R3 New and Changed Features

There are no new features or enhancements to existing features for NFX Series in Junos OS Release 17.3R3.

Release 17.3R2 New and Changed Features

There are no new features or enhancements to existing features for NFX Series in Junos OS Release 17.3R2.

Release 17.3R1 New and Changed Features

Juniper Device Manager

- **Support for Virtual Route Reflector (NFX250-S2)**—Starting in Junos OS Release 17.3R1, you can implement the virtual router reflector capability by creating and deploying a VRR virtual machine as a VNF (Virtual Network Function) on the NFX250-S2 device. Benefits of implementing virtual route reflectors are:
 - Improved scalability
 - Fast and more flexible deployment
 - Savings as a result of elimination of router hardware

SEE ALSO

[Changes in Behavior and Syntax | 224](#)

[Known Behavior | 225](#)

[Known Issues | 225](#)

[Resolved Issues | 226](#)

[Documentation Updates | 226](#)

[Migration, Upgrade, and Downgrade Instructions | 227](#)

[Product Compatibility | 228](#)

Changes in Behavior and Syntax

There are no changes in behavior and syntax for NFX Series in Junos OS Release 17.3R2.

SEE ALSO

[New and Changed Features | 223](#)[Known Behavior | 225](#)[Known Issues | 225](#)[Resolved Issues | 226](#)[Documentation Updates | 226](#)[Migration, Upgrade, and Downgrade Instructions | 227](#)[Product Compatibility | 228](#)

Known Behavior

There are no known limitations in Junos OS Release 17.3R3 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.

SEE ALSO

[New and Changed Features | 223](#)[Changes in Behavior and Syntax | 224](#)[Known Issues | 225](#)[Resolved Issues | 226](#)[Documentation Updates | 226](#)[Migration, Upgrade, and Downgrade Instructions | 227](#)[Product Compatibility | 228](#)

Known Issues

There are no known issues in hardware and software in Junos OS Release 17.3R3 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.

SEE ALSO

New and Changed Features 223
Changes in Behavior and Syntax 224
Known Behavior 225
Resolved Issues 226
Documentation Updates 226
Migration, Upgrade, and Downgrade Instructions 227
Product Compatibility 228

Resolved Issues

There are no fixed issues in Junos OS Release 17.3R3 for NFX Series.

SEE ALSO

New and Changed Features 223
Changes in Behavior and Syntax 224
Known Behavior 225
Documentation Updates 226
Known Issues 225
Migration, Upgrade, and Downgrade Instructions 227
Product Compatibility 228

Documentation Updates

There are no errata or changes in Junos OS Release 17.3R3 documentation for NFX Series.

SEE ALSO

New and Changed Features 223
Changes in Behavior and Syntax 224
Known Behavior 225

[Known Issues | 225](#)

[Resolved Issues | 226](#)

[Migration, Upgrade, and Downgrade Instructions | 227](#)

[Product Compatibility | 228](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 227](#)

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.

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 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL 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 on EEOL releases and to review a list of EEOL releases, see <https://support.juniper.net/support/eol/software/junos/>.

SEE ALSO

New and Changed Features 223
Changes in Behavior and Syntax 224
Known Behavior 225
Documentation Updates 226
Known Issues 225
Resolved Issues 226
Product Compatibility 228

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 228

Hardware Compatibility

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

To determine the features supported on NFX Series in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at: <https://pathfinder.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

New and Changed Features 223
Changes in Behavior and Syntax 224
Known Behavior 225
Documentation Updates 226

[Known Issues | 225](#)

[Resolved Issues | 226](#)

[Migration, Upgrade, and Downgrade Instructions | 227](#)

Junos OS Release Notes for PTX Series Packet Transport Routers

IN THIS SECTION

- [New and Changed Features | 229](#)
- [Changes in Behavior and Syntax | 237](#)
- [Known Behavior | 240](#)
- [Known Issues | 241](#)
- [Resolved Issues | 244](#)
- [Documentation Updates | 249](#)
- [Migration, Upgrade, and Downgrade Instructions | 249](#)
- [Product Compatibility | 254](#)

These release notes accompany Junos OS Release 17.3R3 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.

New and Changed Features

IN THIS SECTION

- [Release 17.3R3 New and Changed Features | 230](#)
- [Release 17.3R2 New and Changed Features | 230](#)
- [Release 17.3R1 New and Changed Features | 230](#)

This section describes the new features and enhancements to existing features in the Junos OS main release and the maintenance releases for PTX Series.

Release 17.3R3 New and Changed Features

There are no new features in Junos OS Release 17.3R3 for PTX Series routers.

Release 17.3R2 New and Changed Features

Software Installation and Upgrade

- **Device serial number added to DHCP option 60 (PTX1000)**—Starting in Junos OS Release 17.3R2, DHCP option 60 (Vendor Class Identifier) includes the serial number of the device when you use Zero Touch Provisioning (ZTP) to automate provisioning of the device configuration and software image. The serial number can uniquely identify the device in a broadcast network. The serial number appears in the format *Juniper-model-number*. For example, a PTX1000 router numbered DA000 appears as *Juniper-ptx1000-DA000*.

Release 17.3R1 New and Changed Features

Class of Service

- **Support for setting the DSCP code point for host-originating IS-IS traffic sent over a GRE tunnel (PTX Series)**—Starting in Junos OS Release 17.3R1, you can determine traffic prioritization for IS-IS traffic originating on a host and being sent over a GRE tunnel by assigning a DSCP code point to the IS-IS packets. You can set the DSCP code point by including the **isis-over-gre dscp-code-point value** statement at the **[edit class-of-service host-outbound-traffic protocol]** hierarchy level.

[See [protocol \(Host Outbound Traffic\)](#).]

- **Support for shaping of the traffic exiting a physical interface (PTX10008)**—Starting with Junos OS Release 17.3R1, you can shape the output traffic of a physical interface on PTX10008 routers so that the interface transmits less traffic than it is physically capable of carrying. Shaping on a PTX10008 router interface has a minimum rate of 1 Gbps and an incremental granularity of 0.1 percent of the physical interface speed after that (for example, 10 Mbps increments on a 10 Gbps interface). You can shape the output traffic of a physical interface by including the **shaping-rate** statement at the **[edit class-of-service interfaces interface-name]** or **[edit class-of-service traffic-control-profiles profile-name]** hierarchy level and applying the traffic control profile to an interface.

[See [shaping-rate \(Applying to an Interface\)](#).]

General Routing

- **Commit process split into two steps (PTX Series)**—Starting in Junos OS Release 17.3R1, new configuration statements are introduced for **commit** to split the commit process into two steps. These configuration statements are **prepare** and **activate**.

In the first step, known as preparation stage, **commit prepare** validates the configurations and then creates the necessary files and database entries so that the validated configurations can be activated at a later stage.

In the second step, referred to as the activation stage, **commit activate** activates the previously prepared commit. A new configuration statement, **prepared**, is added to **clear system commit**, which clears the prepared commit cache

This feature enables you to configure a number of Junos OS devices and simultaneously activate the configurations. This approach is helpful in time-critical scenarios.

[See [Commit Preparation and Activation Overview](#).]

Interfaces and Chassis

- **Management Ethernet interface (fxp0) is confined in a non-default virtual routing and forwarding table (PTX 10008)**—Starting in Junos OS Release 17.3R1, you can confine the management interface in a dedicated management instance by setting a new CLI configuration statement, **management-instance**, at the **[edit system]** hierarchy level. By doing so, operators will ensure that management traffic no longer has to share a routing table (that is, the default.inet.0 table) with other control or protocol traffic in the system. Instead, there is a **mgmt_junos** routing instance introduced for management traffic.

[See [Management Interface in a Non-Default Instance](#) and [management-instance](#).]

- **Support for confining management Ethernet Interface (fxp0) in a virtual routing and forwarding table (PTX10008)**—Starting in Junos OS Release 17.3R1, Junos OS is able to confine the management interface in a dedicated management instance by setting a new CLI configuration statement, **management-instance**, at the **[edit system]** hierarchy level. By doing so, operators will ensure that management traffic no longer has to share a routing table (that is, default.inet.0 table) with other control or protocol traffic in the system. Instead, there is a **mgmt_junos** routing instance introduced for management traffic.

For more information, see [Configuring the mgmt_junos Routing Instance](#)

Management

- **Support to configure YANG files for Junos Telemetry Interface (PTX Series)**—Starting with Junos OS Release 17.3R1, you can add user-defined YANG files that provide mappings between the XML path and the OpenConfig path for data streamed through the Junos Telemetry Interface. Previously, only the Junos OpenConfig package was available for providing these mappings to the XML proxy when streaming data through gRPC. To add YANG files, include the **request system yang add package *package-name* proxy-xml module *yang-file-path*** operational command. You can validate the YANG module by using the **request system yang validate proxy-xml module *yang-file-path*** command. To delete a YANG file, use the **request system yang delete package *package-name* proxy-xml *yang-file-path*** operational command.

[See [Creating YANG Files for XML Proxy for Junos Telemetry Interface](#).]

- **Enhancements to BGP peer sensors for Junos Telemetry Interface (PTX Series)**—Starting with Junos OS Release 17.3R1, telemetry data streamed through gRPC for BGP peers is reported separately for each routing instance. To export data for BGP peers, you must now include the following path in front of all supported paths:

/network-instances/network-instance/[name_ 'instance-name']/protocols/protocol/

Additionally, the following paths are also now supported:

- **/network-instances/network-instance/protocols/protocol/
bgp/neighbors/neighbor/afi-safis/afi-safi/state/prefixes/accepted**
- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/snmp-peer-index**
- **/network-instances/network-instance/protocols/protocol/
bgp/neighbors/neighbor/afi-safis/afi-safi/state/queues/output**
- **/network-instances/network-instance/protocols/protocol
/bgp/neighbors/neighbor/afi-safis/afi-safi/state/queues/input**
- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/state/ImportEval**
- **/network-instances/network-instance/protocols/protocol/
bgp/neighbors/neighbor/state/ImportEvalPending**

Use the **telemetrySubscribe** RPC to specify telemetry parameters and provision the sensor. If your device is running a version of Junos OS with an upgraded FreeBSD kernel, you must download the Junos Network Agent software package, which provides the interfaces to manage gRPC subscriptions.

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

- **Junos Telemetry Interface support for Routing and Control Board RCB-PTX-X6-32G (PTX3000)**—Starting with Junos OS Release 17.3R1, the Routing and Control Board (RCB) on PTX3000 routers supports the Junos Telemetry Interface, which enables you to provision sensors to export telemetry data for various network elements. The RCB combines the functionality of a Routing Engine, Control Board, and Centralized Clock Generator (CCG) in a single FRU. To provision sensors to stream data through UDP, all parameters are configured at the **[edit services analytics]** hierarchy level. To provision sensors to

stream data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters for a specified list of OpenConfig command paths. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models.

[See [Overview of the Junos Telemetry Interface](#).]

- **Enhanced support for Junos Telemetry Interface (PTX1000 routers)**—Starting with Junos OS Release 17.3R1, you can also provision sensors through the Junos Telemetry Interface for the following network elements:

- Logical interfaces, including queue statistics (UDP and gRPC streaming)
- BGP Peers (gRPC streaming only)
- Memory utilization for routing protocol tasks (gRPC streaming only)
- RSVP interface events (gRPC streaming only)
- Firewall filters, including traffic-class counter (UDP and gRPC streaming)
- Chassis components (gRPC streaming only)
- Aggregated Ethernet interfaces configured with the Link Aggregation Control Protocol (gRPC streaming only)
- Ethernet interfaces enabled configured with the Link Layer Discovery Protocol (gRPC streaming only)
- Routing Engine logical and physical interfaces (UDP and gRPC streaming)
- Optical interfaces (UDP and gRPC streaming)
- Network Discovery Protocol table state (gRPC streaming only)
- Address Resolution Protocol table state (gRPC streaming only)
- IPFIX inline flow aggregation (UDP streaming only)

To provision sensors to stream data through UDP, all parameters are configured at the **[edit services analytics]** hierarchy level. To provision sensors to stream data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters for a specified list of OpenConfig command paths. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models.

[See [Overview of the Junos Telemetry Interface](#).]

Multicast

- **Support for next generation MVPN and Internet multicast (PTX1000)**—Starting in Junos OS Release 17.3R1, the **mpls-internet-multicast** routing instance type uses ingress replication provider tunnels to carry IP multicast data between routers through an MPLS cloud, using MBGP (or next generation) MVPN.

NOTE: Next-generation MVPN is supported only when the **enhanced-mode** statement is configured at the **[edit chassis network-services]** hierarchy level.

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

- **Support for next generation MVPN and Internet multicast (PTX10008)**—Starting in Junos OS Release 17.3R1, the **mpls-internet-multicast** routing instance type uses ingress replication provider tunnels to carry IP multicast data between routers through an MPLS cloud, using MBGP (or next generation) MVPN. Next generation MVPN is available only for PTX Series routers that have third-generation FPCs installed.

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

Network Management and Monitoring

- **mLDP MIB extends support to LDP point-to-multipoint (P2MP) LSPs (PTX Series)**—Starting in Junos OS Release 17.3R1, the mLDP MIB builds on the objects and tables that are defined in RFC 3815, which only support LDP point-to-point label switched paths (LSPs). This mLDP MIB provides support for managing multicast LDP point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) LSPs. The mLDP MIB tables are directly accessible through SNMP. All objects in the mLDP MIB are read-only and cannot be created or set through SNMP. This implementation of mLDP MIB is specified in draft-ietf-mpls-mldp-mib.
- **Support for inline jflow version 9 flow templates (PTX1000)**—Starting in Junos OS Release 17.3R1, you can use inline-JFlow's export capabilities with version 9 flow templates to define a flow record template suitable for IPv4 or IPv6 traffic.

[See [Configuring Flow Aggregation to Use Version 9 Flow Templates on PTX Series Routers](#).]

Operation, Administration, and Maintenance

- **Junos OS daemons to natively emit JSON output (PTX Series)**—Starting with Junos OS Release 17.3R1, the operational state emitted by the daemons is supported in JSON format as well as XML format. To configure JSON format, specify the following CLI command: **set system export-format state-data json compact**. To specify JSON format for specific command output, include **display json** in specific CLI commands.
- **Junos OS OpenConfig to support adjacent RIB operational state model (PTX Series)**—Starting with Junos OS Release 17.3R1, **adj-rib-in-pre** and **adj-rib-out-post** tables have been added for the OpenConfig RIB operational state mode. The BGP RIB consists of several tables per address family, consisting of **loc-rib** and **per-neighbor** tables.

Routing Policy and Firewall Filters

- **Optimized performance for DSCP and traffic-class firewall filter match conditions (PTX10008)**—Starting in Junos OS Release 17.3R1, the **promote dscp** and **promote traffic-class** indicators are supported in firewall filters for IPv4 and IPv6 traffic. When either of these are applied to a filter, the entire filter is compiled in a way that optimizes its performance for the **dscp** or **traffic-class** match condition. The indicators are configured at the **[edit firewall family (inet | inet6) filter filter-name]** hierarchy level.

NOTE: Enabling the indicators requires that network services is set to **enhanced-mode**. Use of the indicators may impact the performance of the **source-port** match condition.

- **Optimized performance for DSCP and traffic-class firewall filter match conditions (PTX1000)**—Starting in Junos OS Release 17.3R1, the **promote dscp** and **promote traffic-class** indicators are supported in firewall filters for IPv4 and IPv6 traffic. When either are applied to a filter, the entire filter is compiled in a way that optimizes its performance for the **dscp** or **traffic-class** match condition. The indicators are configured at the **[edit firewall family (inet | inet6) filter filter-name]** hierarchy level.

NOTE: Enabling the indicators requires that network services be set to **enhanced-mode**. Use of the indicators might impact the performance of the **source-port** match condition.

[See [Promote DSCP](#) and [Promote traffic-class](#).]

- **Support for Hop-limit firewall filter match condition (PTX10008)**—Starting in Junos OS Release 17.3R1, you can configure a firewall filter using the **hop-limit hop-limit** and **hop-limit except hop-limit** match conditions for Internet Protocol version 6 (IPv6) traffic (family inet6).

NOTE: The **hop-limit hop-limit** and **hop-limit except hop-limit** match conditions are supported on PTX series routers when you configure the network-services mode as **enhanced-mode** on the router.

For more information, see [Firewall Filter Match Conditions for IPv6 Traffic](#).

- **Hop-limit firewall filter match condition supported (PTX1000)**—Starting in Junos OS Release 17.3R1, you can configure a firewall filter using the **hop-limit** and **hop-limit except** match conditions for IP version 6 (IPv6) traffic (family inet6).

NOTE: The **hop-limit** and **hop-limit except** match conditions are supported on PTX1000 routers when **enhanced-mode** is configured on the router.

[See [Firewall Filter Match Conditions for IPv6 Traffic](#).]

Routing Protocols

- **Routing protocol process (rpd) recursive resolution over multipath (PTX Series)**—Starting in Junos OS Release 17.3R1, when a BGP prefix that has a single protocol next hop is resolved over another BGP prefix that has multiple resolved paths (unilist), all the paths are selected for protocol next-hop resolution. In prior Junos OS releases, only one of the paths is picked for protocol next-hop resolution. This new feature benefits densely connected networks where BGP is used to establish infrastructure connectivity such as WAN networks with high equal-cost multipath and seamless MPLS topology.

To configure recursive resolution over multipath, define a policy that includes the **multipath-resolve** action at the **[edit policy-options policy-statement *policy-name* then]** hierarchy level and import the policy at the **[edit routing-options resolution rib *rib-name*]** hierarchy level.

[See [Configuring Recursive Resolution over BGP Multipath](#).]

- **Support for IS-IS SPRING and RSVP coexistence (PTX Series)**—Starting in Junos OS Release 17.3R1, the routing protocol process (rpd) takes into account the bandwidth used by SPRING traffic to calculate the balance bandwidth available for RSVP-TE. The allocated bandwidth for RSVP is periodically modified based on the traffic on the SPRING interface and its bandwidth utilization. To configure automatic bandwidth calculation, include the **auto-bandwidth template** statement at the **[edit routing-options]** hierarchy level. You can apply the **auto-bandwidth template** configuration either globally at the **[edit protocols isis source-packet-routing traffic-statistics]** hierarchy level or at the **[edit protocols isis interface *interface-name*]** hierarchy level. This feature is useful for networks that are moving to SPRING but also have RSVP deployed, and continue to use both SPRING and RSVP.

[See [auto-bandwidth](#).]

- **Support for BGP Large Communities (PTX Series)**—Starting with Junos OS Release 17.3R1, BGP community is enhanced to support BGP large community that uses 12-byte encoding where the most significant 4 bytes encode autonomous system number or global administrator and the remaining two 4 bytes encode operator defined local values. Currently, BGP normal community (4 byte) and BGP extended community (6 byte) provide limited support for BGP community attributes after the introduction of 4-byte autonomous system number. Configure the large BGP community attributes at the **[edit policy-options community *community-name* members]** hierarchy level and at the **[edit routing-options static route *route* community]** hierarchy level with keyword **large** followed by three 4-byte unsigned integers separated by colons. The attributes are represented as large:autonomous system number:local value 1:local value2.
- **Support for BGP to carry flow-specification routes (PTX10008)**—Starting in Junos OS Release 17.3R1, BGP can carry flow-specification network layer reachability information (NLRI) messages on a PTX10008 router. Propagating firewall filter information as part of BGP enables you to propagate firewall filters against denial-of-service (DoS) attacks dynamically across autonomous systems.

[See [Example: Enabling BGP to Carry Flow-Specification Routes](#).]

Services Applications

- **Support for inline JFlow version 9 flow templates (PTX 10008 routers)**—Starting in Junos OS Release 17.3R1, you can use inline-JFlow export capabilities with version 9 flow templates to define a flow record template suitable for IPv4 or IPv6 traffic.

[See [Monitoring Network Traffic Flow Using Inline Flow Monitoring on PTX Series Routers.](#)]

SEE ALSO

Changes in Behavior and Syntax 237
Known Behavior 240
Known Issues 241
Resolved Issues 244
Documentation Updates 249
Migration, Upgrade, and Downgrade Instructions 249
Product Compatibility 254

Changes in Behavior and Syntax

IN THIS SECTION

- [Forwarding and Sampling | 238](#)
- [Interfaces and Chassis | 238](#)
- [Management | 238](#)
- [Network Management and Monitoring | 238](#)
- [Services Application | 239](#)
- [VLAN-Infrastructure | 240](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 17.3R3 for the PTX Series.

Forwarding and Sampling

- In Junos OS Release 17.3R1, and later, the **SelectorID** field (element id: 302) is sent instead of the **Bytes** field (element id: 1) in the system scope of **version-ipfix** Option template records for all PTX Series Routers. All other elements of the template remain the same.

Interfaces and Chassis

- **Restart FPC option supported on PTX1000 router**—In Junos OS Release 17.3, you can reboot the FPC gracefully using **request chassis fpc restart slot slot-number** command on a PTX1000 router. Note that **request chassis fpc (online|offline) slot slot-number** command is not supported, which means only restart option is supported, but online and offline options are not supported.

[See [request chassis fpc](#).]

Management

- **Changes to custom YANG RPC syntax (PTX Series)**—Starting in Junos OS Release 17.3, custom YANG RPCs have the following changes in syntax:
 - The **junos:action-execute** statement is a substatement to **junos:command**. In earlier releases, the **action-execute** and **command** statements are placed at the same level, and the **command** statement is optional.
 - The CLI formatting for a custom RPC is defined within the **junos-odl:format** statement, which takes an identifier as an argument. In earlier releases, the CLI formatting is defined using a container that includes the **junos-odl:cli-format** statement with no identifier.
 - The **junos-odl:style** statement defines the formatting for different styles within the statement. In earlier releases, the CLI formatting for different styles is defined using a container that includes the **junos-odl:cli-format** and **junos-odl:style** statements.
- **Enhancement to show agent sensors command (PTX Series)** —Starting with Junos OS Release 17.3R1, the **show agent sensors** command, which displays information about Junos Telemetry Interface sensors, displays the default value of **0** for the **DSCP** and **Forwarding-class** values. Previously, the displayed default value for these fields was **255**. The default value is displayed when you do not configure a DSCP or forwarding-class value for a sensor at the **[edit services analytics export-profile profile-name]** hierarchy level.

[See [export-profile](#) and [show agent sensors](#).]

Network Management and Monitoring

- **SNMP syslog messages changed (PTX Series)**—Starting in Junos OS Release 17.3R1, two misleading SNMP syslog messages have been rewritten to accurately describe the events:

- OLD --AgentX master agent failed to respond to ping. Attempting to re-register
NEW -- AgentX master agent failed to respond to ping, triggering cleanup!
- OLD -- NET-SNMP version %s AgentX subagent connected
NEW --- NET-SNMP version %s AgentX subagent Open-Sent!

[See the [MIB Explorer](#).]

- **Enhancement to about-to-expire logic for license expiry syslog messages (PTX Series)**—Starting in Junos OS Release 17.3R1, the logic for multiple capacity type licenses and when their expiry raises alarms was changed. Before, the behavior had alarms and syslog messages for expiring licenses raised based on the highest validity, which would mislead users in the case of a license expiring earlier than the highest validity license. The new behavior has the about-to-expire logic based on the first expiring license.
- **Change in default log level settings (PTX Series)**—Starting in Junos OS Release 17.3R2, the following changes were made to the default logging levels:

Before this change:

- SNMP_TRAP_LINK_UP was LOG_INFO for both the physical (IFD) and logical (IFL) interfaces.
- SNMP_TRAP_LINK_DOWN was LOG_WARNING for both the physical (IFD) and logical (IFL) interfaces.

After this change:

- IFD LinkUp - LOG_NOTICE (although this is an important message, it appears less frequent)
- IFL LinkUp - LOG_INFO (no change)
- IFD and IFL LinkDown - LOG_WARNING (no change)

[See the [MIB Explorer](#).]

Services Application

- **Changes to the show services rpm history-results command (PTX Series)**—Starting in Junos OS Release 17.3R1, you must include the **owner owner** and **test name** options when using the **show services rpm history-results** command.

[See [show services rpm history-results](#).]

- In Junos OS Release 17.3R1 and later, for PIC-based J-Flow on MX Series routers and inline J-Flow on PTX Series routers, the Options template and Options data records include the **Sampling Interval** field as part of the **ScopeTemplate** field instead of the **ScopeSystem** field.

VLAN-Infrastructure

- **LAG interface flaps while adding/removing a VLAN**—Starting in Junos OS Release 17.3, the LAG interface flaps while adding or removing a VLAN. The flapping happens when a low-speed SFP is plugged into a relatively high-speed port. To avoid flapping, configure the port speed to match the speed of the SFP.

SEE ALSO

New and Changed Features 229
Known Behavior 240
Known Issues 241
Resolved Issues 244
Documentation Updates 249
Migration, Upgrade, and Downgrade Instructions 249
Product Compatibility 254

Known Behavior

IN THIS SECTION

- [General Routing | 240](#)
- [MPLS | 241](#)

This section contains the known behavior, system maximums, and limitations in hardware and software in Junos OS Release 17.3R3 for PTX Series.

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

General Routing

- Uneven load balancing of traffic might occur if the traffic stream changes only in the 0-15 bits of the Layer 3 destination IPv6 address. This limitation might not be visible if the other parameters affecting

the load balance change along with L3_DST, such as L3 source IP address, L4 source/destination ports, and so on. [PR1065515](#)

- On a PTX Series router with a faulty power supply module (PSM), the PSM might generate excessive interrupt requests. Because hardware interrupt requests are processed by the chassis process (chassisd), excessive interrupt requests might cause chassisd to restart when the condition persists for more than 200 seconds. [PR1226992](#)

MPLS

- When next-generation MVPN is configured with RSVP provider tunnels and NSR is used, then the egress router for the tunnel might not correctly replicate some of the tunnel state to the backup Routing Engine, leading to temporary traffic loss during NSR failover for the effected tunnels. [PR1293014](#)

SEE ALSO

[New and Changed Features | 229](#)

[Changes in Behavior and Syntax | 237](#)

[Known Issues | 241](#)

[Resolved Issues | 244](#)

[Documentation Updates | 249](#)

[Migration, Upgrade, and Downgrade Instructions | 249](#)

[Product Compatibility | 254](#)

Known Issues

IN THIS SECTION

- [General Routing | 242](#)
- [Interfaces and Chassis | 243](#)
- [Routing Protocols | 243](#)

This section lists the known issues in hardware and software in Junos OS Release 17.3R3 for the PTX Series.

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

General Routing

- In certain transient scenarios, when egress the physical interface is down and ingress is sending still-traffic, **eprq_map_disabled** error messages will be displayed. There is no functional impact because of these messages. [PR1123949](#)
- A PTX Series FPC3 might receive noise on the FPC console port and might interpret it as valid signals. This might cause a login failure on the console port and generate core files or even reloads. [PR1224820](#)
- On rare occasions, upon reboot, the kernel cannot create sysfs entries for the solid-state drives in the system. This might result in the system entering panic mode and hanging. [PR1261068](#)
- When an FPC goes offline or restarts, FPC 'x' sends traffic to FPC 'y'. The following error messages are seen on the destination FPC. A corresponding alarm is set on the destination FPC. Specific to the PTX10000, the transient alarm gets set when this condition occurs. The alarm clears later because the source FPC goes offline. **Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Error (0x210613), module: PE Chip, type: Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Cmerror Op Set: PE Chip: PE1[1]: FO:core intr: 0x00000010: Grant spray drop due to unspray-able condition error Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Error (0x210614), module: PE Chip, type: Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Cmerror Op Set: PE Chip: PE1[1]: FO:core intr: 0x00000008: Request spray drop due to unspray-able condition error** [PR1268678](#)
- Sometimes l2cpd core files are generated when LLDP neighbors are cleared. [PR1270180](#)
- Interfaces might go down when Packet Forwarding Engine encounters **TOE::FATAL ERROR**. The target of evaluation (TOE) is a module in the Packet Forwarding Engine. The fatal error can be caused either by a software issue or hardware issues such as memory parity errors or others. As a workaround, reboot the line card to recover the service when hitting the issue. [PR1300716](#)
- This type of crash indicates simultaneous operation on an ephemeral instance. When a process wants to open ephemeral configuration in merge view, some other activity (such as purging, deletion/recreation) is being carried out on this ephemeral instance. The occurrence of this core is rare. [PR1305424](#)
- On PTX10000 series platform with FPC "LC1101 - 30C / 30Q / 96X" installed, the 10G interface might flap when the interface is active and it is set to 100 Gbps speed. [PR1315079](#)
- On PTX platform, error message could be observed when FPC card goes online or offline. [PR1322491](#)
- On PTX Series platform with broadband cards (for example, FPC1, FPC2) and class-of-service (CoS) used, a high priority queue might not get the entire configured bandwidth. [PR1324853](#)
- When PTX5000 software is upgraded to a Junos OS version, the software upgrade FPC (fully loaded with PICs and optics) might raise the minor chassis alarm "Consumption > 90percent of allocated Budget". [PR1345478](#)

- PTX3000 reports CCL (Chip to Chip Link) CRC errors while FPC3-SFF-PTX-1X is offlined through CLI command or press offline button. The syslog error is generated by an FPC just before it goes offline, so there is no detectable traffic loss. [PR1348733](#)
- On next generation Routing Engine (NG RE), a failure of the Hardware Random Number Generator (HWRNG) will leave the system in a state where not enough entropy is available to operate. [PR1349373](#)
- If firewall filter is configured, in a rare condition, the host interface might be wedged on PTX Series platform with FPC type 3. [PR1354580](#)
- Intermittently few packets are found to be matching on default route with reject NH in forwarding chip, though valid route is present in the FIB. [PR1358363](#)

Interfaces and Chassis

- Junos upgrade involving Junos OS Release 14.2R5 (and above in 14.2 maintenance releases) and Junos OS Release 16.1 above mainline releases with CFM configuration can cause cfmd crash after upgrade. This is due the old version of `/var/db/cfm.db`. [PR1281073](#)

Routing Protocols

- With Shared Risk Link Group (SRLG) enabled under corner conditions, after executing the command **clear isis database**, the rpd might crash because the IS-IS database tree gets corrupted. [PR1152940](#)

SEE ALSO

[New and Changed Features | 229](#)

[Changes in Behavior and Syntax | 237](#)

[Known Behavior | 240](#)

[Resolved Issues | 244](#)

[Documentation Updates | 249](#)

[Migration, Upgrade, and Downgrade Instructions | 249](#)

[Product Compatibility | 254](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 17.3R3 | 244](#)
- [Resolved Issues: 17.3R2 | 246](#)
- [Resolved Issues: 17.3R1 | 248](#)

This section lists the issues fixed in the Junos OS main release and the maintenance releases.

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

Resolved Issues: 17.3R3

General Routing

- On PTX 5000 with FPC type 3 in rare condition, FPC might crash during lo0.0 inet6 input filter. [PR1268875](#)
- Periodic export of IPFIX flow packets with high octet values. [PR1286427](#)
- The routing protocol process (rpd) might generate a core file while restarting the process. [PR1291110](#)
- Repeated log message %PFE-3 fpcX expr_nh_index_tree_ifl_get and expr_nh_index_tree_ipaddr_get are observed when sampling packet is discarded with log (or syslog) knob under firewall filter. [PR1304022](#)
- The **interface hold-time down** timer does not take effect on PTX5000 with optical interface. [PR1307302](#)
- Rpd core is observed after multiple session flaps on scale setup. [PR1312169](#)
- Continuous logs from vhcliclient for all the commands executed. [PR1315128](#)
- The RIB and FIB might get out of synchronization because the KRT asynchronous queue might get stuck. [PR1315212](#)
- After Jack-out/Jack-in FPC's showing up as "No-Power" for some time; FPC however comes up. [PR1319156](#)
- The rpd might crash when OpenConfig package is upgraded with JTI streaming data in the background. [PR1322553](#)
- JSA10864 2018-07 Security Bulletin: Junos OS: MPC7/8/9, PTX-FPC3 (FPC-P1, FPC-P2), PTX3K-FPC3 and PTX1K: Line card might crash upon receipt of specific MPLS packet (CVE-2018-0030). [PR1323069](#)

- On PTX1000, MX204, MX10003 or QFX10002-60C, the local time on FPC might be different from the local time on Junos VM or VM host. [PR1325048](#)
- PTX MKA sessions are not coming up, after changing CA parameters like - transmit-interval, key-server-priority. [PR1325392](#)
- MPLS traceroute fails across PTX Series platform. [PR1327609](#)
- On PTX5k with FPC3 linecards, PTX10k, and PTX1k platforms, output firewall filters that are configured with **syslog** and **discard** actions do not perform the "syslog" action. [PR1328426](#)
- PTX10K line card might reboot continuously after upgrading to Junos OS Release 17.2R1 or above if HMC BIST fails. [PR1330618](#)
- Link instability is observed after link-down event on PTX Series device. [PR1330708](#)
- PTX5K FPC might reboot in certain rare scenarios when **interface-specific policer** is configured. [PR1335161](#)
- Member of IPv4 unicast next hops might be stuck in "Replaced" state after interface flaps. [PR1336201](#)
- Disabling a breakout 10G port on et-0/0/5 will unexpectedly disable another breakout 10G port on et-0/0/5. [PR1337975](#)
- FPC/FPC2/FPC E on PTX does not forward traffic. [PR1339524](#)
- PTX FPC link goes down after router reboot or flap. [PR1340612](#)
- MPLS traceroute for P2MP LSPs configured with link-protection causes FPC crash. [PR1348314](#)
- BFD sessions do not come up on PTX3000. [PR1352112](#)
- Flabels might get exhausted after multiple Routing Engine switch-over. [PR1354002](#)
- The interface of 15 100G ports PIC might delay 60 seconds to come up. [PR1357410](#)
- Routes stuck in krt queue with error 'EINVAL -- Bad parameter in request'. [PR1362560](#)
- The traffic is still forwarded through the member link of an aggregated Ethernet bundle interface even with "Link-Layer-Down" flag set. [PR1365263](#)
- On PTX IPLC (OPT3-SFF-PTX FPC), a first J-UKERN crash triggers multiple secondary J-UKERN crashes. [PR1365791](#)

Infrastructure

- PTX Series device might get to abnormal state due to the malfunction of the protection mechanism for F-Label. [PR1336207](#)

MPLS

- Traffic drop during NSR switchover for RSVP P2MP provider tunnels used by MVPN. [PR1293014](#)
- The rpd might crash on backup Routing Engine due to memory exhaustion. [PR1328974](#)
- MPLS LSP statistics are not shown in CLI command **show mpls lsp ingress statistics**. [PR1344039](#)

Platform and Infrastructure

- PTX1000 and QFX10002-60C: Python scripts/shell scripts cannot be executed during ZTP as veriexec is enabled. [PR1334425](#)
- Traffic black hole is seen along with **JPRDS_NH:jprds_nh_alloc(),651: JNH[0] failed** to grab new region for NH messages. [PR1357707](#)

Routing Protocols

- The rpd might constantly consume high CPU in BGP setup. [PR1315066](#)
- The primary path of MPLS LSP might switch to other address. [PR1316861](#)
- The rpd process might crash continuously on both Routing Engines when **backup-spf-options remote-backup-calculation** is configured in IS-IS protocol. [PR1326899](#)
- Rpd might crash if SRLG information is in the protocol IS-IS. [PR1337849](#)

VPN

- In a specific CE device environment in which asynchronous-notification is used, after the link between the PE and CE devices goes up, the L2 circuit flaps repeatedly. [PR1282875](#)

Resolved Issues: 17.3R2

General Routing

- On PTX1000 routers, the error message **ch_get_product_attribute.324: Cannot find chassisd** is displayed when loading images. [PR1217505](#)
- On PTX Series routers, a faulty power supply module (PSM) might generate excessive interrupt requests. These hardware interrupt requests, processed by chassisd, might restart the chassisd process when the condition persists more than 200 seconds. [PR1226992](#)
- The **validation-state:unverified** routing entry might not be shown with the proper location when users run **show route**. [PR1254675](#)
- The rpd process might crash after BGP sessions and routes flap. [PR1269327](#)
- 100GBase-ER4 (740-045420) is shown as UNKNOWN when the CLI command **show chassis hardware** is executed in Junos OS Release 15.1R5. [PR1280089](#)
- FPC cards might go offline because of fabric healing in a PTX3000 with a SIB-SFF-PTX-240-S platform. [PR1282983](#)
- The MPLS TTL might reset to 255 on third-generation PTX Series FPCs if the **protocols mpls no-propagate-ttl** statement is configured. [PR1287473](#)
- LSP traffic might silently drop and get discarded after a link goes down in bypass path. [PR1291036](#)
- The routing protocol process (rpd) might generate a core file while restarting the process from the CLI. [PR1291110](#)

- Incorrect SNMP OID values are sent in SNMP traps for removal or insertion of a front panel display on PTX Series routers. [PR1294741](#)
- LINK LED is RED when the port is disabled on PTX Series routers. [PR1294871](#)
- The rpd core file is generated after interface or BGP flapping. [PR1294957](#)
- The chassisd process might run out of memory and restart on a PTX1000 platform. [PR1295691](#)
- On a PTX5000 or an Ethernet Synchronization Message Channel (ESMC), the clock does not get locked when the source interface is a member link of an aggregated Ethernet bundle. [PR1296015](#)
- The mgd core file is generated when downgrading from Junos OS Release 17.3-20170721 to Junos OS Release 16.1X65D40.2. The mgd core file is overwritten if downgrading is attempted multiple times. [PR1296504](#)
- On a PTX1000, upgrade from Junos OS Release 16.1X65D45 to Junos OS Release 17.3-20170721 fails frequently with sampling enabled. [PR1296533](#)
- Alarms and syslog errors are seen with priority strict-high on an AF4 queue, on the oversubscription cases (1X100G egress to 1X10G egress setup). [PR1297343](#)
- The disable-pfe action upon Hybrid Memory Cube (HMC) fatal errors might have a system-wide impact on PTX Series platforms. [PR1300180](#)
- PTX Series router FPC3 drops MPLS packets when the maximum transmission unit is less than the MPLS packet size on the outgoing interface with IPv4 traffic. [PR1302256](#)
- Heap memory leak might be observed on PTX Series router FPCs during a multicast route installation into the Packet Forwarding Engine. [PR1302303](#)
- On a PTX3000, powering on an FPC (OPT-3-SFF-PTX/IPLC) card reboots the other FPC cards. [PR1302304](#)
- The third-generation FPC (FPC3-SFF-PTX) might not boot on a PTX3000 with the Control Board or Routing Engine. [PR1303295](#)
- The 100G interfaces might not come up on a PTX3000 and a PTX5000. [PR1303324](#)
- This issue occurs when using MPLS LSPs and RSVP-TE self-ping. When rpd sends out a self-ping packet and an RSVP packet at the same time, these packets might overwrite the kernel's packet buffers causing memory corruption and kernel panic. [PR1303798](#)
- PTX3000 with RCB-PTX Routing Engine might be unable to come online or recognize integrated photonic line cards (IPLCs). [PR1304124](#)
- The routing information base (RIB - also known as routing table) and forwarding information base (FIB - also known as forwarding table) might not synchronize in a large-scale network, because of a timing issue. The root cause is that when the rpd sends route update messages to the kernel, the KRT queue that is used to send the messages can get into a state in which no more messages can be sent to the kernel. [PR1315212](#)
- The physical interfaces might generate framing errors when ports are connected to an odd interface. [PR1317827](#)

Infrastructure

- The **show system users** CLI command output displays more users than that are actually using the router. [PR1247546](#)

Interfaces and Chassis

- 100G interfaces might not come up when **otn-options laser-enable** is configured on PTX Series platforms. [PR1297164](#)
- LFM discovery state might show up as a fault for an aggregated interface after a GRES switchover. [PR1299534](#)

MPLS

- In an RSVP environment, a stale LSP might get created after a Routing Engine switchover with nonstop routing (NSR) enabled. [PR1292526](#)
- The rpd might crash when the MPLS LSP path change occurs. [PR1295817](#)

Platform and Infrastructure

- Continuous log messages occur. For example: **tftpd[23724]: Timeout #35593 on DATA block 85.** [PR1315682](#)

Routing Protocols

- A few BFD sessions flap while coming up after FPC restarts or reboots. [PR1274941](#)
- Multihop BFD sessions flap continuously when the PTX Series router is in the middle hop. [PR1291340](#)
- The rpd process crashes and generates core files multiple times when you receive an OPEN message from an existing BGP peer. [PR1299054](#)
- With BGP labeled unicast MPLS fast reroute in an inter-AS scenario, a very high fast reroute time is visible once the link is up. [PR1307258](#)

Resolved Issues: 17.3R1

Layer 2 Features

- All the XML duplications and unformatted output are addressed. For Example, histogram was just declared as a element inside pfkey container, with this change a new container is defined for histogram. [PR1271648](#)

SEE ALSO

[New and Changed Features | 229](#)

[Changes in Behavior and Syntax | 237](#)

[Known Behavior | 240](#)

[Known Issues | 241](#)

[Documentation Updates | 249](#)

[Migration, Upgrade, and Downgrade Instructions | 249](#)

[Product Compatibility | 254](#)

Documentation Updates

There are no errata or changes in Junos OS Release 17.3R3 documentation for PTX Series.

SEE ALSO

[New and Changed Features | 229](#)

[Changes in Behavior and Syntax | 237](#)

[Known Behavior | 240](#)

[Known Issues | 241](#)

[Resolved Issues | 244](#)

[Migration, Upgrade, and Downgrade Instructions | 249](#)

[Product Compatibility | 254](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 250](#)
- [Upgrading a Router with Redundant Routing Engines | 250](#)
- [Basic Procedure for Upgrading to Release 17.3 | 250](#)

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.

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 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or from Junos OS Release 14.2 to Release 16.1. However, you cannot upgrade directly from a non-EEOL 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://support.juniper.net/support/eol/software/junos/>.

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](#).

Basic Procedure for Upgrading to Release 17.3

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

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

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

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

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 17.3R3:

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 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: After you install a Junos OS Release 17.3R3 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.

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 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.

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

```
user@host> request system software add validate reboot source/jinstall-17.3
R3.SPIN-domestic-signed.tgz
```

All other customers, use the following command:

```
user@host> request system software add validate reboot source/jinstall-17.3
R3.SPIN-export-signed.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** (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.

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 17.3 `jinstall` package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the `jinstall` package that corresponds to the previously installed software.

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

SEE ALSO

New and Changed Features	229
Changes in Behavior and Syntax	237
Known Behavior	240
Known Issues	241
Resolved Issues	244
Documentation Updates	249
Product Compatibility	254

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 254](#)

Hardware Compatibility

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

To determine the features supported on PTX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at: <https://pathfinder.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

New and Changed Features 229
Changes in Behavior and Syntax 237
Known Behavior 240
Known Issues 241
Resolved Issues 244
Documentation Updates 249
Migration, Upgrade, and Downgrade Instructions 249

Junos OS Release Notes for the QFX Series

IN THIS SECTION

- New and Changed Features | 255
- Changes in Behavior and Syntax | 272
- Known Behavior | 276
- Known Issues | 281
- Resolved Issues | 287
- Documentation Updates | 299
- Migration, Upgrade, and Downgrade Instructions | 300
- Product Compatibility | 313

These release notes accompany Junos OS Release 17.3R3 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.

New and Changed Features

IN THIS SECTION

- Release 17.3R3 New and Changed Features | 256
- Release 17.3R2 New and Changed Features | 257
- Release 17.3R1 New and Changed Features | 258

This section describes the new features and enhancements to existing features in the Junos OS main release and the maintenance releases for QFX Series.

NOTE: The following QFX Series platforms are supported in Release 17.3R3: QFX5100, QFX5110, QFX5200, QFX10002, QFX10008, and QFX10016.

Release 17.3R3 New and Changed Features

EVPNs

- **IPv4 inter-VLAN multicast forwarding modes for EVPN (QFX10000 switches)**—Starting with Junos OS Release 17.3R3, QFX10000 switches can forward IPv4 multicast traffic between VLANs in EVPN-VXLAN networks with these IP fabric architectures:
 - Two-layer IP fabric in which QFX10000 switches function as Layer 3 gateways, and QFX5100 or QFX5200 switches function as Layer 2 gateways. From their central location in the IP fabric, the QFX10000 switches on which IRB interfaces are configured can route multicast traffic from one VLAN to another. This mode of multicast forwarding is known as *centrally-routed mode*.
 - One-layer IP fabric in which QFX10000 switches function as both Layer 2 and Layer 3 gateways. From their location at the edge of the IP fabric, the QFX10000 switches on which IRB interfaces are configured can route multicast traffic from one VLAN to another. This mode of multicast forwarding is known as *edge-routed mode*.

To configure the multicast forwarding mode, you can specify the **irb** configuration statement with the **local-remote** option (centrally-routed mode) or the **local-only** option (edge-routed mode) in the **[edit forwarding-options multicast-replication evpn]** hierarchy level.

NOTE: We do not recommend specifying the **local-remote** option on some QFX10000 switches and the **local-only** option on the other QFX10000 switches in either of the IP fabric architectures. Doing so might cause the QFX10000 switches to forward the inter-VLAN multicast traffic inconsistently.

Routing Policy and Firewall Filters

- **Support for packet load balancing based on GTP-TEID hashing (QFX10002, QFX10008, and QFX10016 switches)**—Starting in Junos OS Release 17.3R3-S1, you can configure load balancing of IPv4 or IPv6 packets by using GPRS Tunneling Protocol-tunnel endpoint identifier (GTP-TEID) field hash calculations. The GTP-TEID hashing is added to the Layer 2 and Layer 3 field hashing that you have already configured. To enable this feature, configure the **gtp-tunnel-endpoint-identifier** statement at the **[edit forwarding-options enhanced-hash-key family inet]** or the **[edit forwarding-options enhanced-hash-key family inet6]** hierarchy Level. GTP versions 1 and 2 are supported; they support only user data. You must use UDP port number 2152 for both GTP versions.

Release 17.3R2 New and Changed Features

EVPNs

- **EVPN-VXLAN with MPLS as transport layer (QFX10000 line switches)**—Starting with Junos OS Release 17.3R2, Ethernet VPN-Virtual Extensible LANs (EVPN-VXLANs) are supported with MPLS as the transport layer.

At present, QFX 10000 switches provide Layer 2 and Layer 3 VXLAN gateway functions for bare-metal server (BMS) or Virtual Machines (VMs) connected to it by means of a switch network or top-of-rack through an IRB interface. It also supports inter-DC connectivity via Type-5. The current transport layer support is IP. The feature adds MPLS as a transport for Layer 2 VXLANs with EVPN type-5 gateway functionality only. Layer 3 IRB VXLAN gateways will continue to use IP as the transport layer, even if MPLS is configured.

IP Tunneling

- **IPv6 GRE tunneling support (QFX10002, QFX10008, and QFX10016)**—Starting with Junos OS Release 17.3R2, Junos OS support IPv6 Generic routing encapsulation (GRE) tunnels in QFX10000 line switches..

Multicast

- **Support for next-generation multicast VPN (QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 17.3R2, QFX10002, QFX10008, and QFX10016 switches support Multiprotocol BGP (MBGP) next-generation multicast VPNs with the following provider tunnel types:
 - Ingress replication provider tunnels
 - RSVP-Traffic Engineering (RSVP-TE) point-to-multipoint (P2MP) provider tunnels

- Multipoint LDP P2MP provider tunnels

Virtual Chassis

- **Virtual Chassis support (QFX5200 switches)**—Starting in Junos OS Release 17.3R2, QFX5200-32C switches can be interconnected into a Virtual Chassis as one logical device managed as a single chassis. A QFX5200 Virtual Chassis can contain up to 3 members that must be QFX5200-32C switches, with no mixed mode support. Any non-channelized 40-Gbps QSFP+ ports can be configured as Virtual Chassis ports (VCPs) to interconnect member switches. As of Junos OS Release 17.3R2-S4, 100-Gbps QSFP28 ports can also be configured as Virtual Chassis ports (VCPs).

Configuration and operation are the same as for other QFX Series Virtual Chassis.

[See [Understanding QFX Series Virtual Chassis](#).]

Release 17.3R1 New and Changed Features

Class of Service (CoS)

- **Enhanced Transmission Selection (ETS) support (QFX10000 line switches)**—Beginning with Junos OS Release 17.3R1, ETS is supported on QFX10000 Series devices, compliant with IEEE 802.1Qaz/D0.1. ETS support enables the definition of multiple priority groups at each egress port of the device. Priority queues are combined into priority groups, enabling the application of similar congestion control capabilities to all queues within a group.

[See [Understanding CoS Hierarchical Port Scheduling \(ETS\)](#).]

EVPNs

- **Support of Layer 3 connectivity in an EVPN-VXLAN topology (QFX5110)**—Starting with Junos OS Release 17.3R1, you can deploy a QFX5110 switch as a Layer 3 Virtual Extensible LAN (VXLAN) gateway in an EVPN-VXLAN topology with a two-layer IP fabric or an IP fabric that is collapsed to one layer. In this role, the QFX5110 switch provides Layer 3 connectivity between physical (bare-metal) servers and virtual machines (VMs) within a data center. On QFX5110 switches, you can configure integrated routing and bridging (IRB) interfaces that route packets between VLANs. While creating an IRB interface, you can configure the interface as a default Layer 3 gateway, which physical servers in one VLAN use to communicate with physical servers or VMs in another VLAN.

[See [Example: Configuring a QFX5110 Switch as a Layer 3 VXLAN Gateway in an EVPN-VXLAN Topology with a Two-Layer IP Fabric](#) and [Example: Configuring a QFX5110 Switch as Layer 2 and 3 VXLAN Gateways in an EVPN-VXLAN Topology with a Collapsed IP Fabric](#).]

- **Support for multiple routing instances of type Virtual Switch and EVPN, VLAN-based service on the EVPN routing instance, and VLAN-aware service on the Virtual Switch routing instance (QFX10000 line switches)**—Starting with Junos OS Release 17.3R1, you can configure both EVPN and Virtual Switch routing instances. EVPN routing instance supports VLAN-based service. It includes only a single broadcast domain and there is a one-to-one mapping between a VNI and MAC-VRF. Up to 100 EVPN routing instances are supported. The Virtual Switch instance supports VLAN-aware service, and up to 10 Virtual

Switch routing instances are supported. Each Virtual Switch routing instance can have up to 4094 VLANs, but the total number of VLANs across the Virtual Switch routing instances cannot exceed the system limitation.

NOTE: If you create VLANs that are not part of a routing instance, they become part of the Default Switch routing instance.

- **EVPN Proxy ARP and ARP Suppression (QFX10000 line switches)**—Starting with Junos OS Release 17.3R1, QFX10000 switches that function as provider edge (PE) devices in an Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) environment support proxy Address Resolution Protocol (ARP) and ARP suppression. The proxy ARP and ARP suppression capabilities are enabled by default. For both features to work properly, the configuration of an integrated and routing (IRB) interface on the PE device is required.

IRB interfaces configured on a PE device deliver ARP requests from both local and remote customer edge (CE) devices. When a PE device receives an ARP request from a CE device, the PE device searches its media access control (MAC)-IP address bindings database for the requested IP address. If the PE device finds the MAC-IP address binding in its database, it responds to the request. If the device does not find the MAC-IP address binding, it swaps the source MAC address in the request with the MAC address of the IRB interface on which the request was received and sends the request to all interfaces.

Even when a PE device responds to an ARP request, ARP packets might still be flooded across the WAN. ARP suppression prevents this flooding from occurring.

[See [EVPN Proxy ARP and ARP Suppression](#).]

- **Support for external multicast router for EVPN with IGMP snooping (QFX10000)**—Starting with Junos OS Release 17.3R1, you can configure a provider edge (PE) switch running Ethernet VPN (EVPN) to send and receive multicast traffic to an external multicast router. This implementation supports the forwarding of inter-VLAN multicast traffic without having to configure IRB interfaces. Traffic is forwarded through a Layer 3 multicast protocol such as Protocol Independent Multicast (PIM). To enable the PE switch to receive multicast traffic from the multicast router, include the **multicast-router-interface** statement at the **[edit protocols igmp-snooping vlan *vlan-name* interface *interface-name*]** hierarchy level.

Support for forwarding inter-VLAN and intra-VLAN multicast traffic in an EVPN-VXLAN environment with IRB interfaces was introduced on QFX10000 switches in Junos OS Release 17.2R1.

[See [multicast-router-interface \(IGMP Snooping\)](#).]

- **Support for external Layer 3 multicast device for EVPN with IGMP snooping (QFX10000)**—Starting with Junos OS Release 17.3R1, you can connect an Ethernet VPN (EVPN) provider edge switch to an external Layer 3 device running a multicast protocol such as Protocol Independent Multicast (PIM). In this implementation, one or more provider edge switches configured with EVPN are connected to an external, that is, gateway, multicast device through a Layer 2 VLAN. To enable the PEs to forward traffic to the external domain, configure PIM-to-IGMP translation by including the **pim-to-igmp-proxy**

upstream-interface *irb-interface-name* statements at the **[edit routing-options multicast]** hierarchy level. Additionally, this implementation supports configuring PIM on the IRB interfaces on the PE so that it functions only to forward inter-VLAN traffic within the data center. This means that you do not need to configure a PIM rendezvous point because forming PIM adjacencies is not required. The gateway device only needs to view the data center as a Layer 2 multicast domain. Include the new **passive** statement at the **[edit protocols pim]** hierarchy level to configure PIM to perform only inter-VLAN forwarding of multicast traffic.

[See [Overview of IGMP Snooping in an EVPN-VXLAN Environment](#).]

General Routing

- **Commit process split into two steps (QFX Series)**—Starting in Junos OS Release 17.3R1, new configuration statements are introduced for **commit** to split the commit process into two steps. These configuration statements are **prepare** and **activate**.

In the first step, known as preparation stage, **commit prepare** validates the configurations and then creates the necessary files and database entries so that the validated configurations can be activated at a later stage.

In the second step, referred to as the activation stage, **commit activate** activates the previously prepared commit. A new configuration statement, **prepared**, is added to **clear system commit**, which clears the prepared commit cache

This feature enables you to configure a number of Junos OS devices and simultaneously activate the configurations. This approach is helpful in time-critical scenarios.

[See [Commit Preparation and Activation Overview](#).]

High Availability (HA) and Resiliency

- **Support for VRRP over IRB interfaces (QFX5100 Virtual Chassis and Virtual Chassis Fabric)**—Starting in Junos OS Release 17.3R1, you can configure Virtual Router Redundancy Protocol Version 3 (VRRPv3) for an IPv4 or IPv6 IRB interface on a QFX5100 Virtual Chassis or Virtual Chassis Fabric (VCF). The Virtual Chassis or VCF can act as the master or backup switch in a VRRP group, and the IRB interface forwards traffic sent to the configured VRRP virtual address that corresponds to the default gateway for the VLAN. Use the **vrrp-group** or **vrrp-inet6-group** configuration statement in the [edit interfaces irb unit *logical-unit-number* family (inet | inet6) address *address*] statement hierarchy on the Virtual Chassis or VCF as part of the IRB interface configuration.

[See [Configuring Basic VRRP Support for QFX](#) and [Configuring IRB Interfaces](#).]

Interfaces and Chassis

- **Increased number of link aggregation groups (LAGs) (QFX10008 and QFX10016 switches)**—Starting with Junos OS Release 17.3R1, you can configure up to 1000 LAGs on QFX10008 and QFX10016 switches. To configure, include the **device-count** statement with a value of 1000 at the [edit chassis aggregated-devices ethernet] hierarchy level and add member links in each bundle.
- **Short-reach mode (QFX5100-48T switch)**—Allows you to use short cable lengths (less than 10 meters) for copper-based 10-Gigabit Ethernet interfaces. Enabling short-reach mode reduces power consumption on these interfaces. You can configure short-reach mode for individual interfaces and for a range of interfaces. Enable short-reach mode for individual interfaces by including the enable statement at the [edit chassis fpc <slot-number> pic <slot-number>] hierarchy. Enable short-reach mode for a range of interfaces by including the enable statement at the [edit chassis fpc <slot-number> pic port-range <port low> <port high>] hierarchy.
- **IEEE 1588v2 Precision Time Protocol (PTP) Boundary Clock (QFX10002 switches)**—Starting with Junos OS Release 17.3R1, a boundary clock, which has multiple network connections, can act as a source

(master) or destination (slave) for synchronization messages. The boundary clock intercepts and processes all Precision Time Protocol (PTP) messages and passes all other traffic. The best master clock algorithm (BMCA) is used by the boundary clock to select the best clock from configured acceptable masters. You can configure a port as a boundary slave or as a boundary master. To configure a boundary clock, include the **boundary** statement at the **[edit protocols ptp clock-mode]** hierarchy level.

[See [IEEE 1588v2 PTP Boundary Clock Overview](#).]

- **Auto-channelization of interfaces (QFX5200 switch)**—Starting in Junos OS Release 17.3, you can use the auto-channelization feature to divide and channelize data automatically by detecting the cable type. The mode and number of channels are decided based on the channel link status. On QFX5200, auto-channelization supports three modes of operation with unique port settings:
 - When 4x10G split cables are connected, the 40G port auto-channelizes to four 10G channels.
 - When 2x50G split cables are connected, the 100G port auto-channelizes to two 50G channels.
 - When 4x25G split cables are connected, the 100G port auto-channelizes to four 25G channels.
- **Support for static link protection on aggregated interfaces (QFX5100 switches)**—Starting in Junos OS Release 17.3R1, you can enable link protection on a specified static label-switched paths (LSP). You can designate a primary and a backup physical link to support link protection. Egress traffic passes only through the designated primary link. This includes transit traffic and locally generated traffic on the router. When the primary link fails, traffic is routed through the backup link.

See [Configuring Node Protection or Link Protection for LSPs](#).

- **Support for consistent load balancing for ECMP groups (QFX10000 line switches)**—Starting with Junos OS Release 17.3R1 on QFX10000 switches, you can prevent the reordering of flows to active paths in an ECMP group when one or more paths fail. Only flows that are on inactive paths are redirected. This feature applies only to Layer 3 adjacencies learned through external BGP connections. It overrides the default behavior of disrupting all existing, including active, TCP connections when an active path fails. Include the **consistent-hash** statement at the **[edit policy-options policy-statement policy-statement-name then load-balance]** hierarchy level. You must also configure a global per-packet load-balancing policy.

[See [Understanding Consistent Load Balancing Through Resilient Hashing on ECMP Groups](#).]

- **CL74 FEC support for 25-gigabit and 50-gigabit channel speeds (QFX5200 switches)**—Starting with Junos OS Release 17.3, you can disable or reenabling clause 74 (CL74)—as well as CL91—forwarding error correction (FEC) support on QFX5200 switches. FEC CL91 is supported for the 100-gigabit port speed and FEC CL74 is supported for both 25-gigabit and 50-gigabit port speeds. FEC CL91 is enabled by default for the 100-gigabit port speed; when the ports are channelized either in 4x25-gigabit or 2x50-gigabit, FEC CL74 is enabled.
 - To disable the FEC mode:

```
[edit]
set interfaces interface-name together-options fec none
```

- To reenable the FEC mode:

```
[edit]
delete interfaces interface-name gigether-options fec none
```

or

```
[edit]
set interfaces interface-name gigether-options fec (fec74|fec91)
```

- To check FEC status:

```
show interfaces interface-name
```

The output for the show command will list FEC statistics for a particular *interface-name*, including the FEC corrected errors count, the FEC uncorrected errors count, and the type of FEC that was disabled or enabled.

Layer 2 Features

- **Support to exclude IRB Interfaces from state calculations (QFX5100)**—Starting with Junos OS Release 17.3R1, you can exclude a trunk or access interface from the state calculations for an IRB interface for member VLANs. An IRB interface typically has multiple ports in a single VLAN. Excluding trunk and access interfaces from state calculations means that as that soon as the port specifically assigned to the VLAN goes down, the the IRB interface for the VLAN is marked as down. Include the **autostate-exclude** statement at the **[edit interfaces ether-options]** hierarchy level. This feature was previously introduced in Junos OS Release 14.1X53-D40.

[See [Excluding an IRB Interface from State Calculations](#).]

- **Increases number of vmembers to 256k for integrated routing and bridging interfaces and aggregated Ethernet interfaces (QFX10000 line switches)**—To calculate vmember utilization, multiply the number of VLANS assigned to a port by the number of ports. The number should be less than or equal to 256k.

Management

- **Enhancements to BGP peer sensors for Junos Telemetry Interface (QFX5110, QFX5200, and QFX10000)**—Starting with Junos OS Release 17.3R1, telemetry data streamed through gRPC for BGP peers is reported separately for each routing instance. To export data for BGP peers, you must now include the following path in front of all supported paths:
/network-instances/network-instance/[name_ 'instance-name']/protocols/protocol/

Additionally, the following paths are also now supported:

- `/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi/state/prefixes/accepted`
- `/network-instances/network-instance/protocols/protocol/bgp/neighbors/snmp-peer-index`
- `/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi/state/queues/output`
- `/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi/state/queues/input`
- `/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/state/ImportEval`
- `/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/state/ImportEvalPending`

Use the **telemetrySubscribe** RPC to specify telemetry parameters and provision the sensor. If your device is running a version of Junos OS with an upgraded FreeBSD kernel, you must download the Junos Network Agent software package, which provides the interfaces to manage gRPC subscriptions.

[See [Guidelines for gRPC Sensors](#).]

- **Support for LSP events and properties sensor for Junos Telemetry Interface (QFX5110 and QFX5200)**—Starting with Junos OS Release 17.3R1, you can export statistics for LSP events and properties through the Junos Telemetry Interface. Only gRPC streaming for this sensor is supported. You can export statistics for ingress point-to-point LSPs, point-to-multipoint LSPs, bypass LSPs, and dynamically created LSPs. To export data through gRPC, use the `/mpls/lsp/` or `/mpls/signal-protocols/` set of OpenConfig subscription paths. Use the **telemetrySubscribe** RPC to specify telemetry parameters and provision the sensor. If your device is running a version of Junos OS with an upgraded FreeBSD kernel, you must download the Junos Network Agent software package, which provides the interfaces to manage gRPC subscriptions. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models. This sensor was previously supported only on QFX10000 switches, MX Series routers, and PTX Series routers.

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

- **Support for the Junos Telemetry Interface (QFX5110)**—Starting with Junos OS Release 17.3R1, you can provision sensors through the Junos Telemetry Interface to export telemetry data for various network elements without involving polling on QFX5110 switches. Only gRPC streaming of statistics is supported on QFX5110 switches. UDP streaming is not supported.

The following sensors are supported:

- BGP peers
- RSVP interface events

- Memory utilization for routing protocol tasks
- Label-switched-path events and properties
- Ethernet interfaces enabled with the Link Layer Discovery Protocol

To provision sensors to stream data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters for a specified list of OpenConfig commands paths. You must download the Junos Network Agent software package, which provides the interfaces to manage gRPC subscriptions. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models.

Support for the Junos Telemetry Interface was introduced on QFX10000 and QFX5200 switches in Junos OS Release 17.2R1.

[See [Overview of the Junos Telemetry Interface](#).]

Multicast

- **Support for static multicast route leaking for VRF and virtual-router instances (QFX5100 switches)**—Starting with Junos OS Release 17.3R1, you can configure your switch to share IPv4 multicast routes among different virtual routing and forwarding (VRF) instances or different virtual-router instances. Only multicast static routes with a destination-prefix length of /32 are supported for multicast route leaking. Only Internet Group Management Protocol version 3 is supported. To configure multicast route leaking for VRF or virtual-router instances, include the **next-table routing-instance-name.inet.0** statement at the **[edit routing-instances routing-instance-name routing-options static route destination-prefix/32]** hierarchy level. For **routing-instance-name**, include the name of a VRF or virtual-router instance. This feature was initially introduced in Junos OS Release 14.X53-D40.

[See [Understanding Multicast Route Leaking for VRF and Virtual-Router Instances](#).]

MPLS

- **Support for Layer 2 circuit on aggregate interfaces (QFX10000 switches)**—Starting in Junos OS release 17.3R1, you can configure a Layer 2 circuit on aggregate interfaces. You can apply input and output VLAN tags for pop, swap, and push label operations on the VLAN-CCC interface. VLAN tags are applied when traffic is sent to and from the Layer 2 circuit interface. These operations are performed only on the outer TAG. The pop VLAN tag removes the VLAN tag from the top of the VLAN tag stack. The push VLAN tag adds a new outer VLAN tag, and the swap VLAN tag replaces the existing outer VLAN tag with the new VLAN tag. This feature provides interoperability between Layer 2 services with a distinct VLAN at the local or remote end, or for instances where the Layer 2 service comes with a certain VLAN, but the remote peer has a different VLAN or no VLAN.

[See [CCC Overview](#) .]

- **VRF support in IRB interfaces in a Layer 3 VPN (QFX5100 and QFX5100 Virtual Chassis)**—Starting in Junos Release 17.3R1, you can configure IRB interfaces under virtual routing and forwarding (VRF) in a VPN Layer 3 network. IRB interfaces enable a switch to recognize which packets are being sent to local addresses so that they are bridged whenever possible and are routed only when needed. This same

functionality applies, when IRB interfaces are part of routing instances or VRF. Virtual routing instances allows you to divide the switch into multiple independent virtual routers, each with its own routing table. This increases functionality by allowing network paths to be segmented without using multiple devices. Because traffic is automatically segregated, VRF also increases network security and can eliminate the need for encryption and authentication. Internet service providers often take advantage of VRF to create separate VPNs for their customers.

[See [Understanding Virtual Routing and Forwarding Tables](#) .]

- **Support for BGP MPLS-based Ethernet VPN (QFX10000 switches)**—Starting with Junos OS Release 17.3R1, you can use MPLS-based Ethernet VPN (EVPN) to route MAC addresses using BGP over an MPLS core network. An EVPN enables you to connect dispersed customer sites using a Layer 2 virtual bridge. As with other types of VPNs, an EVPN consists of customer edge (CE) devices (host, router, or switch) connected to a provider edge (PE) router or switch. The QFX10000 acts as a PE switch at the edge of the MPLS infrastructure. The switch can be connected by an MPLS Label Switched Path (LSP) which provides the benefits of MPLS technology, such as fast reroute and resiliency. You can deploy multiple EVPNs within a service provider network, each providing network connectivity to a customer while ensuring that the traffic sharing on that network remains private.

[See [EVPN Overview](#).]

Operation, Administration, and Maintenance

- **Junos daemons to natively emit JSON output (QFX Series)**—Starting with Junos OS Release 17.3R1, the operational state emitted by the daemons is supported in JSON format as well as XML format. To configure JSON format, specify the following CLI command: **set system export-format state-data json compact**. To specify JSON format for specific command output, include **display json** in specific CLI commands.
- **Junos OpenConfig to support operational models for VLANs (QFX Series)**—Starting with Junos OS Release 17.3R1, support has been added for an OpenConfig YANG model for VLANs via the addition of **openconfig-vlan.yang**, revision 1.0.2. This provides a unified view for the network agent to retrieve operational state from JUNOS daemons for VLANs.

Port Security

- **MAC-limiting support (QFX10000 switches)**—Starting in Junos OS Release 17.3R1, you can configure MAC limiting on QFX10000 line switches. MAC limiting enhances port security by limiting the number of MAC addresses that can be learned within a VLAN. Limiting the number of MAC addresses protects the switch from flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). Flooding occurs when the number of new MAC addresses that are learned causes the Ethernet switching table to overflow, and previously learned MAC addresses are flushed from the table. The switch then reverts to flooding the previously-learned MAC addresses, which can impact performance and introduce security vulnerabilities.

This feature was previously supported in an “X” release of Junos OS.

[See [Understanding MAC Limiting and MAC Move Limiting for Port Security](#).]

- **IP source guard (QFX5100, QFX5110, QFX5200)**—Starting with Junos OS Release 17.3R1, you can configure the IP source guard access port security feature to mitigate the effects of source IP address spoofing and source MAC address spoofing. If IP source guard determines that a host connected to an access interface has sent a packet with an invalid source IP address or source MAC address in the packet header, it discards the packet.

[See [Understanding IP Source Guard for Port Security on EX Series Switches.](#)]

Routing Protocols Policy and Firewall Filters

- **Flexible Ethernet Support (QFX10000 switches)**—Starting in Junos OS release 17.3R1, you can configure inet, inet6, or vlan-circuit cross-connect (CCC) connections on a physical or aggregate ethernet interface. This allows you to set different forwarding rules for tagged and untagged traffic on the same interface. For example, you can forward tagged packets over the l2circuit and route untagged traffic normally in the native vlan mode.

All logical devices that are under the flexible vlan tagging are identified by their vlan-id configuration. For untagged traffic, the association to the corresponding logical device is derived using the native vlan id configuration on the physical device. For traffic without a vlan tag, the default vlan id (native vlan id) is used to derive the layer2 domain.

Routing Protocols

- **Support for BGP Large Communities (QFX Series)**—Starting with Junos OS 17.3R1, BGP community is enhanced to support BGP large community that uses 12-byte encoding where the most significant 4-bytes encode autonomous system number or global administrator and the remaining two 4-bytes encode operator defined local values. Currently, BGP normal community (4-byte) and BGP extended community (6-byte) provide limited support for BGP community attributes after the introduction of 4-byte autonomous system number. Configure the large BGP community attributes under **[edit policy-options community community-name members]** hierarchy level and under **[edit routing-options static route route community]** hierarchy level with keyword **large** followed by three 4-byte unsigned integers separated by colons. The attributes are represented as large:autonomous system number:local value 1:local value2.
- **Support for segment routing for IS-IS (QFX5110 and QFX5200)**—Starting with Junos OS Release 17.3R1, you can advertise MPLS labels through IS-IS to support segment routing. IS-IS advertises a set of segments, which enables an ingress device to steer a packet through a specific set of nodes and links in the network without relying on the intermediate nodes in the network to determine the path to take. Two types of segments are supported: node and adjacency. A node segment represents a shortest-path link to a node. An adjacency segment represents a specific adjacency to a node. To enable segment routing, include the source-packet-routing statement at the **[edit protocols isis]** hierarchy level. By default, segment routing is enabled on all IS-IS levels. To disable advertising of the adjacency segment for a specified interface, include the no-advertise-adjacency-segment statement. You can also specify an interval for maintaining adjacency segments by including the adjacency-segment hold-time milliseconds statement.

To enable node segments, include the node-segment statement at the **[edit protocols isis source-packet-routing]** hierarchy level. You have two options for advertising a range of indices for IPv4

or IPv6 addresses. Use the **index-range** statement to specify a dynamic label range managed by MPLS. To specify a specific block of indices, also known as a segment routing global block, include the **start-label index-range** statements at the **[edit protocols isis source-packet-routing srgb]** hierarchy level. This configuration enables MPLS to reserve the specified label range. Segment routing in IS-IS also supports provisioning prefix segment indices (SIDs) and anycast SIDs for both IPv4 and IPv6 prefixes. These SIDs are provisioned through a routing policy for each prefix. Include the **prefix-segment index number** statement at the **[edit policy options policy-statement policy-name then]** hierarchy level. You can also enable IPG shortcuts for prefix segment routes. Include the **shortcuts** statement at the **[edit protocols isis traffic-engineering family (inet-mpls | inet6-mpls)]** hierarchy level.

This feature was introduced on QFX5100 and QFX10000 switches in Junos OS Release 17.2R1.

[See [Understanding Source Packet Routing](#).]

- **BGP precision-timer support for reducing BGP hold-time (QFX5100, QFX5100 Virtual Chassis, QFX5110, QFX5200, QFX10000)**—Starting in Junos OS Release 17.3R1, you can use BGP precision timers to enable BGP sessions to send frequent keepalive messages with hold times as short as 10 seconds. The hold time is the maximum time allowed to elapse between successive keepalive messages that BGP receives from a peer. The default hold time is 90 seconds; the default frequency for keepalive messages is 30 seconds. More frequent keepalive messages and shorter hold times might be desirable in large-scale deployments with many active sessions. When you set a **hold-time** value to less than 20 seconds, we recommend that you also configure the BGP **precision-timers** statement, so that if scheduler slip messages occur, the routing device continues to send keepalive messages. When the **precision-timers** statement is included, keepalive messages are generated in a dedicated kernel thread, thus helping to prevent BGP session flaps.

[See [precision-timers](#).]

- **Support for 128 equal-cost paths for BGP multipath (QFX10000)**—Starting with Junos OS Release 17.3R1, you can configure a maximum of 128 equal-cost paths for external BGP peers. Previously, the maximum number supported was 64. For MPLS routes, the maximum number of equal-cost paths you can configure remains unchanged at 64. To specify 128 equal-cost paths for external BGP peers, include the **maximum-ecmp 128** statement at the **[edit chassis]** hierarchy level. You must also configure a routing policy that exports routes from the routing table into BGP. Define a routing policy by including the **policy-statement policy-name** set of statements at the **[edit policy-options]** hierarchy level. Apply the policy to routes exported to the forwarding table by including the **export policy-name** statement at the **[edit routing-options forwarding-table]** hierarchy level.

[See [maximum-ecmp](#).]

NOTE: This feature is released but not supported in Junos OS Release 17.3R1.

- **Support for segment routing for OSPF (QFX5110 and QFX5200)**—Starting with Junos OS Release 17.3R1, you can advertise MPLS labels through OSPF to support segment routing. Only IPv4 is supported. OSPFv3 is not supported. OSPF advertises a set of segments, which enables an ingress device to steer

a packet through a specific set of nodes and links in the network without relying on the intermediate nodes in the network to determine the path to take. Two types of segments are supported: node and adjacency. A node segment represents a shortest-path link to a node. An adjacency segment represents a specific adjacency to a node. To enable segment routing, include the **source-packet-routing** statement at the **[edit protocols ospf]** hierarchy level. By default, segment routing is enabled for all OSPF areas. To disable for a specific area, include the **no-source-packet-routing** statement at the **[edit protocols ospf area area-id]** hierarchy level. To enable node segments, include the **node-segment** statement. You can specify a range for IPv4 addresses to advertise, which MPLS manages dynamically. To disable advertising of the adjacency segment for a specified interface, include the **no-advertise-adjacency-segment** statement.

This feature was introduced on QFX5100 and QFX10000 switches in Junos OS Release 17.2R1.

[See [source-packet-routing](#).]

- **Support for alternate loop-free routes for IS-IS and OSPF (QFX10000)**—Starting in Junos OS Release 17.3R1, this feature adds fast reroute capability for IS-IS and OSPF. Junos OS precomputes loop-free backup routes for all IS-IS or OSPF routes. These backup routes are preinstalled in the Packet Forwarding Engine, which performs a local repair and implements the backup path when the link for a primary next hop for a particular route is no longer available. A loop-free path is one that does not traverse the router to reach a given destination. That is, a neighbor that already forwards traffic to the router is not used as a backup route to that destination.

You can enable support for alternate loop-free routes on any IS-IS or OSPF interface. To provide this support automatically for LDP label-switched paths (LSPs), you must also enable LDP on any interface for which you enabled support for loop-free alternate routes. In addition, you can extend backup coverage to include RSVP LSP paths.

Junos OS provides two mechanisms to enable fast reroute for IS-IS or OSPF using alternate loop-free routes: link protection and node-link protection. When you enable link protection or node-link protection on an IS-IS or OSPF interface, the software creates an alternate path to the primary next hop for all destination routes that traverse a protected interface. Link protection offers per-link traffic protection. It supports fast rerouting of user traffic over one mission-critical link. Node-link protection establishes an alternate path through a different router altogether.

[See [Loop-Free Alternate Routes for OSPF Overview, Example: Configuring Link and Node Protection for IS-IS Routes](#).]

- **Support for alternate loop-free routes for IS-IS and OSPF (QFX5110 and QFX5200)**—Starting in Junos OS Release 17.3R1, this feature adds fast reroute capability for IS-IS and OSPF. Junos OS precomputes loop-free backup routes for all IS-IS or OSPF routes. These backup routes are preinstalled in the Packet Forwarding Engine, which performs a local repair and implements the backup path when the link for a primary next hop for a particular route is no longer available. A loop-free path is one that does not traverse the router to reach a given destination. That is, a neighbor that already forwards traffic to the router is not used as a backup route to that destination.

You can enable support for alternate loop-free routes on any IS-IS or OSPF interface. To provide this support automatically for LDP label-switched paths (LSPs), you must also enable LDP on any interface

for which you enabled support for loop-free alternate routes. In addition, you can extend backup coverage to include RSVP LSP paths.

Junos OS provides two mechanisms to enable fast reroute for IS-IS or OSPF using alternate loop-free routes: link protection and node-link protection. When you enable link protection or node-link protection on an IS-IS or OSPF interface, the software creates an alternate path to the primary next hop for all destination routes that traverse a protected interface. Link protection offers per-link traffic protection. It supports fast rerouting of user traffic over one mission-critical link. Node-link protection establishes an alternate path through a different router altogether.

[See [Loop-Free Alternate Routes for OSPF Overview](#), [Example: Configuring Link and Node Protection for IS-IS Routes](#).]

- **Support for BGP link-state distribution extensions for segment routing (QFX5110 and QFX5200)**—Starting in Junos OS Release 17.3R1, BGP link-state distribution extensions export segment-routing topology information to software-defined networking controllers. Although controllers can obtain the topology information by either being a part of an interior gateway protocol (IGP) domain or through BGP link-state distribution, the latter provides a more scalable mechanism for exporting this information. BGP link-state distribution is supported on inter-domain networks. This feature is useful in networks that are moving to segment routing at the transport layer but also have RSVP deployed. Include the **ipv4-prefix** statement at the **[edit policy-options policy-statement *policy-name* term *term-name* from traffic-engineering]** hierarchy level. This feature was introduced in Junos OS Release 17.2R1 on MX Series and PTX Series routers and on QFX5100 and QFX10000 switches.

[See [Link-State Distribution Using BGP Overview](#).]

- **Routing protocol process (rpd) recursive resolution over multipath (QFX Series)**—Starting in Junos OS Release 17.3R1, when a BGP prefix that has a single protocol next hop is resolved over another BGP prefix that has multiple resolved paths (unilist), all the paths are selected for protocol next-hop resolution. In prior Junos OS releases, only one of the paths is picked for protocol next-hop resolution. This new feature benefits densely connected networks where BGP is used to establish infrastructure connectivity such as WAN networks with high equal-cost multipath and seamless MPLS topology.

To configure recursive resolution over multipath, define a policy that includes the **multipath-resolve** action at the **[edit policy-options policy-statement *policy-name* then]** hierarchy level and import the policy at the **[edit routing-options-resolution rib *rib-name*]** hierarchy level.

[See [Configuring Recursive Resolution over BGP Multipath](#).]

Virtual Chassis

- **Virtual Chassis and Virtual Chassis Fabric (VCF) support (QFX5110)**—Starting with Junos OS Release 17.3R1, QFX5110 switches can be interconnected into a Virtual Chassis or VCF and operate as one logical device managed as a single chassis, as follows:

- QFX5110 Virtual Chassis: Up to 10 members, all QFX5110 switches or in combination with QFX5100 switches. We recommend using QFX5110 switches in the master and backup Routing Engine roles, and QFX5100 switches only in the linecard role.
- QFX5110 VCF: Up to 20 members, all QFX5110 switches or in combination with QFX5100 switches. Spine members must be QFX5110-32Q switches.
- A QFX5110 Virtual Chassis or VCF can contain QFX5110-32Q, QFX5110-48S, QFX5100-24Q, QFX5100-48S, and QFX5100-98S switches. The same software image runs on QFX5110 or QFX5100 switches in a Virtual Chassis or VCF, and you do not need to configure the switches into mixed mode.



CAUTION: Any QFX5100 switches running a “-qfx-5-” Junos OS software image *must* first be upgraded to a “-qfx-5e-” image (using the USB method) to successfully join a mixed QFX5110 Virtual Chassis or VCF.

- Any (non-channelized) 100-Gbps or 40-Gbps QSFP28 ports, 40-Gbps QSFP+ ports, or 10-Gbps SFP+ ports can be Virtual Chassis ports (VCPs).

[See [Understanding QFX Series Virtual Chassis](#) and [Understanding QFX Virtual Chassis Fabric Components](#).]

SEE ALSO

[Changes in Behavior and Syntax | 272](#)

[Known Behavior | 276](#)

[Known Issues | 281](#)

[Resolved Issues | 287](#)

[Documentation Updates | 299](#)

[Migration, Upgrade, and Downgrade Instructions | 300](#)

[Product Compatibility | 313](#)

Changes in Behavior and Syntax

IN THIS SECTION

- Class of Service (CoS) | 272
- EVPNs | 272
- General Routing | 273
- Interfaces and Chassis | 273
- Management | 273
- Network Management and Monitoring | 274
- Routing Policy and Firewall Filters | 275
- Virtual Chassis | 275
- VLAN Infrastructure | 275

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 17.3R3 for the QFX Series.

Class of Service (CoS)

- When you configure a **transmit-rate**, you must also configure a **guaranteed-rate** at **traffic-control-profiles**. If you commit a configuration of a **transmit-rate** without a **guaranteed-rate**, a warning message is displayed and the default scheduler map is applied.

EVPNs

- On QFX10000 switches running Junos OS Release 17.3R3 or later, the local preference setting for an Ethernet VPN (EVPN) pure type-5 route is inherited by IP routes that are derived from the EVPN type-5 route. Further, when selecting an IP route for incoming traffic, the QFX10000 switches consider the local preference of the route. A benefit of the QFX10000 switches including local preference in their route selection criteria is that you can set up a policy to manipulate the local preference, thereby controlling which route the switch selects.
- By default, QFX10000, QFX5100, QFX5110, QFX5200, and QFX5210 switches that act as spine and leaf devices in an EVPN-VXLAN overlay network implement the core isolation feature. If one of these QFX switches loses all of its EVPN internal BGP (IBGP) peering sessions, the core isolation feature, working in conjunction with Link Aggregation Control Protocol (LACP), automatically brings down all Layer 2 Ethernet Switch Identifier (ESI) link aggregation group (LAG) interfaces on the switch. In some

situations, this feature produces an undesired outcome that you can prevent by disabling the feature with the **no-core-isolation** configuration statement at the **[edit protocols evpn]** hierarchy level.

[See [Understanding When to Disable EVPN-VXLAN Core Isolation.](#)]

General Routing

- **Support for deletion of static routes when the BFD session goes down (QFX Series)**—Starting with Junos OS Release 17.3R1, the default behavior of the static route at the **[edit routing-options static static-route bfd-admin-down]** hierarchy level is active. So, the static routes are deleted when the BFD receives a session down message.

[See [Enabling BFD on Qualified Next Hops in Static Routes for Route Selection.](#)]

Interfaces and Chassis

- Starting with Junos OS Release 17.3R3, on QFX5100 switches, the configuration statement **source-destination-only-loadbalancing** under the **[edit forwarding-options enhanced-hash-key]** hierarchy is not visible in the CLI. The statement is not supported on QFX5100.

Management

- **Changes to custom YANG RPC syntax (QFX Series)**—Starting in Junos OS Release 17.3, custom YANG RPCs have the following changes in syntax:
 - The **junos:action-execute** statement is a substatement to **junos:command**. In earlier releases, the **action-execute** and **command** statements are placed at the same level, and the **command** statement is optional.
 - The CLI formatting for a custom RPC is defined within the **junos-odl:format** statement, which takes an identifier as an argument. In earlier releases, the CLI formatting is defined using a container that includes the **junos-odl:cli-format** statement with no identifier.
 - The **junos-odl:style** statement defines the formatting for different styles within the statement. In earlier releases, the CLI formatting for different styles is defined using a container that includes the **junos-odl:cli-format** and **junos-odl:style** statements.
- **Enhancement to show agent sensors command (QFX Series)**—Starting with Junos OS Release 17.3R1, the **show agent sensors** command, which displays information about Junos Telemetry Interface sensors, displays the default value of **0** for the **DSCP** and **Forwarding-class** values. Previously, the displayed default value for these fields was **255**. The default value is displayed when you do not configure a DSCP or forwarding-class value for a sensor at the **[edit services analytics export-profile profile-name]** hierarchy level.

[See [export-profile](#) and [show agent sensors](#).]

Network Management and Monitoring

- **Enhancement to about-to-expire logic for license expiry syslog messages (QFX Series)**—As of Junos OS Release 17.3R1, the logic for multiple capacity type licenses and when their expiry raises alarms was changed. Before, the behavior had alarms and syslog messages for expiring licenses raised based on the highest validity, which would mislead users in the case of a license expiring earlier than the highest validity license. The new behavior has the about-to-expire logic based on the first expiring license.
- **SNMP syslog messages changed (QFX Series)**—In Junos OS Release 17.3R1, two misleading SNMP syslog messages have been rewritten to accurately describe the event:
 - OLD --AgentX master agent failed to respond to ping. Attempting to re-register
NEW -- AgentX master agent failed to respond to ping, triggering cleanup!
 - OLD -- NET-SNMP version %s AgentX subagent connected
NEW --- NET-SNMP version %s AgentX subagent Open-Sent!

[See the [MIB Explorer](#).]

- **Change in default log level setting (QFX Series)**—In Junos OS Release, 17.3R2, the following changes were made in default logging levels:

Before this change:

- SNMP_TRAP_LINK_UP was LOG_INFO for both the physical (IFD) and logical (IFL) interfaces.
- SNMP_TRAP_LINK_DOWN was LOG_WARNING for both the physical (IFD) and logical (IFL) interfaces.

After this change:

- IFD LinkUp -> LOG_NOTICE (since this is an important message but less frequent)
- IFL LinkUp -> LOG_INFO (no change)
- IFD and IFL LinkDown -> LOG_WARNING (no change)

See the [MIB Explorer](#).

- **New context-oid option for trap-options configuration statement to distinguish the traps which come from a non-default routing instance and non-default logical system (QFX Series)**—In Junos OS Release 17.3R3, a new option, **context-oid**, for the **trap-options** statement allows you to handle prefixes such as <routing-instance name>@<trap-group> or <logical-system name>/<routing-instance name>@<trap-group> as an additional varbind.

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

- **Reconfigure SNMPv3 configuration after upgrade (QFX Series)**—Starting in Junos OS Release 17.3R1, you might need to reconfigure SNMPv3 after upgrading from an earlier release. This is necessary only if you are using SNMPv3 and if the engine ID is based on the MAC address because the engine ID has changed. Previously, customers had to reconfigure SNMPv3 after every reboot. This problem was fixed. If you upgrade, you must still reconfigure SNMPv3, but only once. If you have already reconfigured SNMPv3 in an earlier release, then you do not need to reconfigure SNMPv3 again. To reconfigure SNMP

v3, use the **delete snmp v3** command, commit, and then reconfigure SNMPv3 parameters. Platforms affected are QFX5100, QFX10002, QFX10008, and QFX10016.

[See [Configuring the Local Engine ID](#).]

Routing Policy and Firewall Filters

- **Support for configuring the GTP-TEID field for GTP traffic (QFX5100, QFX5110, and QFX5200 switches)**—Starting in Junos OS Release 17.3R3, the **gtp-tunnel-endpoint-identifier** statement is supported to configure the hash calculation of IPv4 or IPv6 packets that are included in the GPRS tunneling protocol–tunnel endpoint identifier (GTP-TEID) field hash calculations. The **gtp-tunnel-endpoint-identifier** configuration statement is configured at the **[edit forwarding-options enhanced-hash-key family inet]** hierarchy level.

In most of the cases, configuring **gtp-tunnel-endpoint-identifier** statement is sufficient for enabling GTP hashing. After enabling, if GTP hashing does not work, it is recommended to capture the packets using relevant tools and identify the offset value. As per standards, 0x32 is the default header offset value. But, due to some special patterns in the header, offset may vary to say 0x30, 0x28, and so on. In this cases, use **gtp-header-offset** statement to set a proper offset value. Once the header offset value is resolved, run **gtp-tunnel-endpoint-identifier** command for enabling GTP hashing successfully.

[See [gtp-tunnel-endpoint-identifier](#) and [gtp-header-offset](#).]

Virtual Chassis

- **Adaptive load balancing (ALB) feature (Virtual Chassis Fabric)**—Starting in Junos OS Release 17.3R2, the adaptive load balancing (ALB) feature for Virtual Chassis Fabric (VCF) is being deprecated to avoid potential VCF instability. The **fabric-load-balance** configuration statement in the **[edit forwarding-options enhanced-hash-key]** hierarchy is no longer available to enable and configure ALB in a VCF. When upgrading a VCF to a Junos OS release where ALB is deprecated, if the configuration has ALB enabled, you should delete the **fabric-load-balance** configuration item before initiating the upgrade.

[See [Understanding Traffic Flow Through a Virtual Chassis Fabric](#) and [fabric-load-balance](#).]

VLAN Infrastructure

- **LAG interface flaps while adding/removing a VLAN**—From Junos OS Release 17.3 or later, the LAG interface flaps while adding or removing a VLAN. The flapping happens when a low speed SFP is plugged into a relatively high speed port. To avoid flapping, configure the port speed to match the speed of the SFP.

SEE ALSO

New and Changed Features	255
Known Behavior	276
Known Issues	281
Resolved Issues	287
Documentation Updates	299
Migration, Upgrade, and Downgrade Instructions	300
Product Compatibility	313

Known Behavior

IN THIS SECTION

- Class of Service (CoS) | 277
- EVPN | 277
- High Availability (HA) and Resiliency | 278
- Layer 2 Features | 278
- MPLS | 278
- Platform and Infrastructure | 279
- Routing Protocols | 280
- Virtual Chassis | 280

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 17.3R3 for the QFX Series.

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

Class of Service (CoS)

- On QFX10000 line switches, oversubscribing all 8 queues configured with the **transmit rate exact** statement at the `[edit class-of-service schedulers scheduler-name]` hierarchy level might result in less than 100 percent utilization of port bandwidth.

[See [transmit-rate](#).]

EVPN

- A provider edge (PE) device running EVPN IRB with an IGP configured in a VRF associated with the EVPN instance will be unable to establish an IGP adjacency with a CE device attached to a remote PE device. The IGP instance running in the VRF on the PE might be able to discover the IGP instance running on the remote CE through broadcast or multicast traffic, but will be unable to send unicast traffic directly to the remote CE device. [PR977945](#)
- On QFX10000 switches configured as type-5 route peers, when only peer 1 advertises routes, that peer might not install the decapsulated next-hop (NH) route. As a result, type-5 encapsulated traffic sent by peer 2 is dropped until peer 2 advertises any type-5 route. As a workaround, configure a static route pointing to discard on peer 2 and advertise that route as a type-5 route to peer 1. [PR1191092](#)
- A QFX10000 switch running Junos OS Release 17.3Rx software might experience a small and continuous traffic loss under the following conditions:
 - The switch is configured as a Layer 2 and/or Layer 3 VXLAN gateway in an EVPN-VXLAN topology with either a two-layer or collapsed IP fabric.
 - The switch has default ARP and MAC aging timer values.

Under these conditions, the following types of traffic flows might be impacted:

- Bidirectional Layer 3 traffic in a multihomed topology.
- Unidirectional Layer 3 traffic in a single-homed topology.

Note that this issue does not impact bidirectional Layer 3 traffic in a single-homed topology.

To prevent loss in these traffic flows, you must set the **aging-timer** configuration statement in the `[edit system arp]` hierarchy level so that the value is less than the value of the **global-mac-table-aging-time** configuration statement in the `[edit protocols l2-learning]` hierarchy level. [PR1309444](#)

- With VXLAN configured for 30 VXLAN VNIs, L3 Unicast traffic loss might be observed on deleting and adding back all the VXLAN VNIs. [PR1318045](#)
- Deleting a EVPN-VXLAN tenant causes scheduler slippage and BFD flap. [PR1366032](#)
- When the vxlan VNI is removed at remote PE device, the flood groups are cleaned up and the MAC routes are deleted. The router continues to accept traffic for the duration the remote node sends traffic to the VNI that is cleaned up. The show commands will reflect the VNI as valid until the tunnel to the remote PE device is deleted. No operational impact. [PR1366983](#)

High Availability (HA) and Resiliency

- During a nonstop software upgrade (NSSU) on an QFX5100 Virtual Chassis, a traffic loop or loss might occur if the Junos OS software version that you are upgrading and the Junos OS software version that you are upgrading to use different internal message formats. [PR1123764](#)

Layer 2 Features

- On QFX5100 Virtual Chassis interfaces on which flexible VLAN tagging has been enabled, STP, RSTP, MSTP, and VSTP protocols are not supported. [PR1075230](#)
- In EVPN-VXLAN deployment with QFX10000 switches, when vxlan enabled IRB interface is configured in the same routing instance as that of the the underlay vtep tunnel and if the remote VTEP interface IP is resolved over the IRB interface using routing protocols or static route, dc-pfe cores would be generated and all the interfaces would go down. dc-pfe cores would be continuously generated until configuration is corrected. [PR1261824](#)
- When the replication tree used for flooding is reconverging, because some of the leaves have been deleted or added, there is expected to be some transient traffic loss even in leaves that have not changed. This affects only flooding and BUM traffic, not known unicast traffic. [PR1274950](#)
- When NG-MVPN is configured with RSVP provider tunnels and NSR is used, then the egress router for the tunnel might not correctly replicate some of the tunnel state to the backup routing engine, leading to temporary traffic loss during NSR failover for the affected tunnels. [PR1293014](#)

MPLS

- On QFX5100, QFX5110, QFX5200 switches with Layer 2 circuit configured on the PE switches, enabling VLAN bridge encapsulation on a CE interface drops packets if flexible Ethernet services and VLAN CCC encapsulation are configured on the same logical interface. You can configure only one encapsulation type, either **set interfaces xe-0/0/18 encapsulation flexible-ethernet-services** or **set interfaces xe-0/0/18 encapsulation vlan-ccc**. [PR1329451](#)
- Layer 2 circuit on aggregated Ethernet (AE) interfaces is not supported on QFX5100, QFX5110, and QFX5200 switches. [PR1333730](#)
- When an analyzer is configured on a QFX5100 switch in the egress direction, packets at the output of analyzer might contain incorrect 802.1q vlan tags. [PR1032512](#)

Platform and Infrastructure

- On EX4600 and QFX5100 switches, the amount of time that it takes for Zero Touch Provisioning to complete might be lengthy because TFTP might take a long time to fetch required data. [PR980530](#)
- On an EX4300 or a QFX5100 Virtual Chassis, when you perform an NSSU, there might be more than five seconds of traffic loss for multicast traffic. [PR1125155](#)
- On QFX10008 switches, if you reboot a QFX10000-36Q line card or a QFX10000-30C line card with traffic running, sometimes framing errors are displayed in the CLI output. This is only a display issue. No actual framing errors have occurred, and traffic is unaffected. [PR1223330](#)
- For a LAG interface, PFE populates only the bundle statistics and not the child's IFL statistics. It always returns zero for IFL statistics. There is a limitation in the hardware which restricts the per IFL stats [PR1250870](#)
- If port speed is changed in from 25G to 100G or there are repeated changes in port speed settings, then the link may remain down. This is a SDK limitation and has been addressed in Broadcom SDK versions 6.5.8 and above. [PR1250891](#)
- On the QFX10K-12C-DWDM Coherent Line Card, when an interface is configured in 8QAM mode, pull out of fiber on the second "OT" interface in the same AC400 module brings both the "OT" interfaces down. This does not affect any functionality. [PR1258539](#)
- Multiple instances of the **DAEMON-3-JTASK_SCHED_SLIP** system message might be logged when over 50,000 MACs are configured and the device attempts to establish OSPF neighbors. This has no functional impact. [PR1274706](#)
- On a QFX5110-32C switch, if a splitter cable is connected to a Spirent 10G CV/MX card, ports will not come up due to varied pre-empt settings for the splitter and DAC cables. There is a hardware limitation where we have no way in EEPROM to differentiate between splitter and DAC cable to apply different settings. As a workaround, use a 40G Spirent card with internal channelization on the Spirent side and manual channelization on the QFX5110-32C side. [PR1280593](#)
- ERPS convergence takes time after GRES switchover and hence traffic loss is observed for a brief period. [PR1290161](#)
- On QFX10000 line platforms, with a high scale of 4000 VNIs or 200K MACs or both, if large configuration change happens with traffic flowing, then forwarding descriptor memory corruption might occur, leading to complete traffic loss on certain ports. The qualification shows that a system with 400 VNIs has been stable. However, other configurations like global MAC count and underlying MPLS LSPs can increase system load. [PR1296089](#)
- Port LEDs on QFX5100 do not work. If a device connects to a port on QFX5100, the port LED stays unlit. [PR1317750](#)
- For QFX5110, there is a hardware limitation. QFX5110 can route from VxLAN (VFI) domain to VxLAN (VFI) domain only, does not support routing from VxLAN domain to non-VxLAN domain. [PR1318178](#)

- When checking BUM traffic statistics on the VTEP, it might show that the traffic is flooding back to the other VTEPs. This is because the statistics is calculated earlier in the pipeline before the packets are actually dropped. This is a statistics issue due to a BRCM pipeline design and has no functionality impact. This is applicable to all Junos OS releases where VXLAN is supported. [PR1348662](#)
- DLR MAC does not age out when **global-mac-table-aging-time** is set to 60 seconds. [PR1367911](#)

Routing Protocols

- The QFX5100 switches do not support Bidirectional Forwarding Detection (BFD) timer values of less than 1 second. If a timer value less than 1 second is configured, it might cause BFD flapping. [PR942035](#)
- During a graceful Routing Engine switchover (GRES) on QFX10000 switches, some IPv6 groups might experience momentary traffic loss. This issue occurs when IPv6 traffic is running with multiple paths to the source, and the join-load-balance statement for PIM is also configured. [PR1208583](#)
- A QFX5110 switch running Junos OS Release 17.3R1 or later software functions as both a Layer 3 VXLAN gateway and a DHCP relay in an EVPN-VXLAN topology. After a DHCP client receives and later releases an IP address on an EVPN-VXLAN integrated routing and bridging (IRB) interface configured on the QFX5110 switch, the binding between the DHCP client and the IP address might not be deleted. As a result, the next time that the DHCP client requests an IP address, the response from the DHCP server might take a few minutes. [PR1261483](#)
- QFX5110: Traffic loss of routed packets might be seen through a non-collapsed EVPN-VxLAN L3 GW, when disjoint VxLANs with IRB are provisioned and unprovisioned in bulk on it." [PR1276423](#)
- Remotely received traffic is not flooded to an access concentrator on FPC 1 when FPC 0 is offlined. [PR1290500](#)
- An adjacency segment identifier will not be created for IPv6-only configured interfaces. If the adjacency uses IP alone or IP+IPv6, then an IPv4 adjacency segment identifier or IPv6 adjacency segment identifier will be created. If the adjacency only uses IPv6, then no adjacency segment identifier will be created. [PR1290515](#)
- A QFX10000 switch running Junos OS Release 17.3Rx or 17.4Rx software might experience a small and continuous traffic loss under the following conditions: 1) The switch is configured as a Layer 2 and/or Layer 3 VXLAN gateway in an EVPN-VXLAN topology with either a two-layer or collapsed IP fabric, and 2) The switch has default ARP and MAC aging timer values. Under these conditions, the following types of traffic flows might be impacted: 1) Bidirectional Layer 3 traffic in a multihomed topology, and 2) Unidirectional Layer 3 traffic in a single-homed topology. Note that this issue does not impact bidirectional Layer 3 traffic in a single-homed topology. [PR1309444](#)

Virtual Chassis

- For a large VC, topology hash might have a good impact on VC stability as it reduces programming by skipping some route for intermediate topologies. However, it could delay traffic switch as we observed.

By default, topology hash is on. There is hidden cli (**set virtual-chassis no-topology-hashF**) to turn it off. [PR1296196](#)

- L2/L3 traffic drop is seen after rebooting whole VC (10 member) or changing VC member list (for example, making 6 VC member from 10 VC, back to 10 member VC). [PR1314429](#)

SEE ALSO

[New and Changed Features | 255](#)

[Changes in Behavior and Syntax | 272](#)

[Known Issues | 281](#)

[Resolved Issues | 287](#)

[Documentation Updates | 299](#)

[Migration, Upgrade, and Downgrade Instructions | 300](#)

[Product Compatibility | 313](#)

Known Issues

IN THIS SECTION

- [Class of Service \(CoS\) | 282](#)
- [EVPN | 282](#)
- [General Routing | 282](#)
- [Interfaces and Chassis | 285](#)
- [Layer 2 Features | 285](#)
- [Network Management and Monitoring | 286](#)
- [Routing Protocols | 286](#)
- [Software Installation and Upgrade | 287](#)

This section lists the known issues in hardware and software for the QFX Series switches in Junos OS Release 17.3R3.

Class of Service (CoS)

- On QFX5110-32C switches, throughput as per RFC 2544 is not 100 percent for some of the frame sizes when the switch is configured with mixed 10/40/100G speed ports. It is fine when tested individually with 10-Gigabit Ethernet, 40-Gigabit Ethernet, and 100-Gigabit Ethernet ports separately. [PR1256671](#)

EVPN

- Mac-move-shutdown stops working if “physical-loop” is introduced continuously in quick succession of 10 mins. Issue is not happening every time but can happen only if “physical-loop” is introduced atleast 4 times. If the loops are spanned over long time, the issue was not seen. The test was performed to check the overall impact on basic features. There was no issue seen on basic learning or major impact on any protocol. This is negative scenario and unlikely to happen in customer network where the multiple loops happen in a short time span. [PR1284315](#)
- A new option **exclusive-mac** is added under protocols l2-learning global-mac-move as follows: **set protocols l2-learning global-mac-move exclusive-mac <mac>**. [PR1285749](#)
- In an EVPN-VXLAN scenario, a previously learned MAC address from a remote Ethernet segment Identifier (ESI) cannot be changed to local even if it is connected directly. The MAC address of the host might remain as learned from ESI instead of the local interface until the MAC address is aged out. [PR1303202](#)
- ARP gets deleted and re-learned during the first ARP refresh with EVPN-VXLAN multihomed CE. So traffic drops and recovers for the first ARP refresh. [PR1327062](#)
- In a scaled EVPN-VXLAN setup, loading the scaled configuration and the base configuration alternately for a few times, can result in losing adjacency and hence the protocols will be down. [PR1349659](#)
- The Packet Forwarding Engine process might crash some times when deleting the Layer 2 VXLAN Association and adding the VXLAN to IRB. This is timing issue so core is seen very rarely. [PR1373621](#)
- The BGP and EVPN tables being out of synchronization. This issue might be related to the policy logic or policy configuration used. Routes that are in the BGP table are not appearing in the instance table. [PR1374072](#)

General Routing

- While using SSH to log in to a VNF the error message **Unrecognized command** is seen. This error has no impact on the functionality. [PR1108785](#)
- On a QFX5100 Virtual Chassis, the MAC address is not learned on an aggregated Ethernet interface configured as a VXLAN Layer 2 port and with the interface mode configured as access. The issue is observed only with aggregated Ethernet interfaces that span multiple Virtual Chassis members and when the member node is rebooted or power cycled. [PR1112790](#)

- While scaling beyond 2000 VLANs or IRBs , Layer 3 multicast traffic does not converge to 100 percentage and continuous drops are observed after bringing down or bringing up the downstream interface or while an FPC comes online after FPC restart. [PR1161485](#)
- When per-packet load balancing is removed or deleted, next hop index may change. [PR1198092](#)
- The ICCP session is maintained by multihop BFD (non-distributed mode). The time interval for BFD keepalive messages is similar to a GRES configuration (for example, keepAlive = 8 seconds). [PR1230576](#)
- On a QFX5110-48S switch, a Gigabit Ethernet interface goes down and comes back up once on a peer as part of a reboot. [PR1237572](#)
- On QFX5100-48T with short-reach mode enabled on copper ports, these copper ports will flap when you commit any configuration related to routing instances. [PR1248611](#)
- Single-bit and multiple-bit ECC errors are not logged on QFX5110 switches. [PR1251917](#)
- On the QFX10000-12C-DWDM coherent line card, it is possible that sometimes the link flaps when MACsec is enabled on Ethernet interfaces. [PR1253703](#)
- The management process might crash if the Openconfig package is installed immediately or within minutes of Network Agent package installation. This is a transient issue and will not impact any functionality. As a workaround, install Openconfig before installing Network Agent. [PR1265815](#)
- The flexible VLAN tagged interface allows both primary and secondary VLAN configuration on different logical units of the same interface, but might not work as expected. [PR1267160](#)
- This issue is applicable to all Virtual Chassis and Virtual Chassis Fabric combinations on the QFX5100, QFX5110, EX4300, and EX4600 platforms. If the reboot option is used with a large Virtual Chassis, some members might not be able to reboot. As a result, some members will still be running the old image and some members will be upgraded to the new image; this causes Virtual Chassis instability. [PR1273271](#)
- No CPU usage is shown in output for **show chassis fpc x** (x= QFX5100) in a mixed Virtual Chassis Fabric. CPU utilization values show 0, because the values are being normalized. CPU utilization value increases if the idle time decreases to some extent. [PR1274665](#)
- A hostname synchronization issue occurs between the Junos OS VM instance and the Linux host on TVP platforms. [PR1283710](#)
- On QFX5100 switches, static LAG link protection switchover/revert is not working consistently. [PR1286471](#)
- When link protection with the backup port state "down" and LACP are configured, sometimes the primary port state goes down without a trigger event and the backup port comes up and begins handling traffic. [PR1297596](#)
- When link protection with the backup port state "down" and LACP are configured, if the backup state "down" is removed from the configuration, both ports should come up and the primary port should pass all egress traffic. In some instances, however, traffic might pass through the backup port instead of the primary port. [PR1297597](#)

- Port 0 of Qfx5100-48t does not come up in mixed VCF. As a workaround, use **phy diag xe0 dsc** command from the BCM shell upon reboot that brings up the port and stays up continuously until the next reboot. [PR1323323](#)
- Family Ethernet-switching cannot be used when flexible VLAN tagging is configured. It is not supported. The behavior is non-deterministic with this configuration and there is a possibility that the dcpfe process generates core files. [PR1316236](#)
- When configuring multihomed EVPN or MC LAG, use the same AE# or configure the same admin-key to make sure the port-ids from both the uplink devices are identical. Otherwise, only one side will come up. [PR1324554](#)
- The management process (mgd) might panic after modifying aggregated Ethernet interface members under "ethernet-switching vlan" stanza. After the mgd panic, the remote session is terminated. [PR1325736](#)
- VIP address cannot be pinged from back-up when VRRP is configured on subinterfaces on QFX10000. [PR1338256](#)
- Commit error observed if the device is downgraded from Junos OS Release 18.2 to Junos OS Release 17.3R3. On loading the new image, certain stale symlinks from previous image contents need to be removed which impact mgd. In this case, the .slax script symlinks from /var/db/sripts/translation are not getting removed, which causes issues in the initial commit by mgd. The issue is only seen when the previous image was having translation scripts (as part of Junos image) and the new image isn't have these translation scripts [PR1355542](#)
- A VC split is happening because the pfed process generates core files and crashes. As a workaround, before initiating NSSU, check if pfed generates core files and crashes. If yes monitor pfed process and start it if it does not run. Then perform NSSU. [PR1362781](#)
- In QFX5100, if a scaled config involving lag interface, 3000+ vlans, and corresponding NHs is removed and new config involving lag interface is applied same time then new config may not take effect till previous config delete is complete. FXPC may take high cpu for prolonged time till delete of previous config is complete. Not observed any other impact on system. [PR1363896](#)
- On QFX10008, QFX10016, PTX5000, PTX10008, PTX10016 platforms, MPLS EXP rewrite is not working properly when the child members of an aggregate interface are in different FPCs [PR1364391](#)
- After a host stops sending traffic, its entries clear when its MAC address times out later. Sometimes IPv6 neighbor entry does not clear right away. There should be no functional impact since the host had already stopped sending traffic. The system eventually recovers when IPv6 neighbor entry times out. [PR1368311](#)
- Before NSSU is initiated, it is recommended to cleanup the storage to avoid unexpected behavior because of storage full. [PR1370573](#)
- On QFX10K platforms, the maximum number of ESI IFLs was 4000 in the Packet Forwarding Engine. The Packet Forwarding Engine process might crash above this limit. [PR1371414](#)
- There are 3 vlans V1001, V1002 and V1003. V1001 is deleted and V1002's VLAN ID and VNI is changed to that of V1001 and a new vlan V1200 is added with the VLAN ID and VNI of vlan V1002. After the

above changes, V1200 is not created in the Packet Forwarding Engine and the other 2 VLANs are functioning as expected. The reason for the new VLAN not created is because, since the new VLAN needs to be created with the same VLAN ID as that of V1002, the `bd_add` for this VLAN is coming before the VLAN V1002 is updated with the VLAN ID of V1001. As a work around, add the `bd` again in the next commit. [PR1371611](#)

- BGP session bounce might sometimes cause not to flood BUM traffic to all remote VTEPs. [PR1373093](#)
- When IRB is deactivated or activated on a spine, some of the ARP/ND entries go missing on it. The entries on other remote spines remain in-tact. After restarting l2-learning on the spine where configuration change was made, the issue gets resolved. [PR1374339](#)

Interfaces and Chassis

- On QFX5100 switches, with MAC and ARP inside an IFA block, an error message that states that an IRB interface and an aggregated Ethernet logical interface do not belong to the same routing instance might be displayed, even though they do belong to the same routing instance. [PR1239191](#)
- The CLI allows you to configure more than 2048 sub-interfaces on LAG interface from Junos OS Release 17.2R1 but it should not be accepted and CLI should block it. [PR1361689](#)

Layer 2 Features

- On a QFX5110 platform with VXLAN configured, when any packet goes out of an underlay L3 interface, VXLAN encapsulated packets might be sent with a VLAN tag and might be dropped at the remote VTEP end. [PR1271708](#)
- When using PTP BC applications on QFX10002, the forwarding path for a directly connected device is not automatically present and is not triggered by the PTP packets generated by the QFX10002. As a workaround, either create the forwarding entries by configuring a routing protocol such as OSPF on the interface or add a static ARP entry for the remotely connected PTP device. [PR1275327](#)
- On QFX10016, after deleting and re-adding of 1000 LAG interfaces, traffic drops are seen until ARP are refreshed even when all the LAG interfaces comes up. [PR1289546](#)
- On QFX5000 platforms, when scaled configuration (with greater than 3000 bridge domains and greater than 8000 ESI FILS) is overwritten with Functional configuration (with 4 bridge domains and lesser than 10 ESI IFLs), using the **load override** command, approximately 2 minutes is taken for cleanup and adding of new configuration. Without waiting for 2 minutes, if overwrite of the configuration is done multiple times, then some bridge domains are not cleaned up in CLI. [PR1363410](#)

Network Management and Monitoring

- The default syslog level is LOG_NOTICE in the default configuration. SNMP_TRAP_LINK_UP for the physical interface (IFD) is logged as LOG_INFO from day one. To help debug physical link UP issues, SNMP_TRAP_LINK_UP events will be logged by default. [PR1287244](#)

Routing Protocols

- On QFX10000 line switches, traffic drop is seen with IS-IS version 6 traffic during convergence in either of the following two scenarios: 1) While doing port unshutdown (that is, bringing up the ports after bringing them down). 2) While FPC comes online after doing an FPC restart. This behavior is seen while flapping one of the IS-IS version 6 sessions. [PR1190180](#)
- On QFX10000 line platforms, during a route next-hop churn or earliest deadline first (EDF), job priority changes, and memory corruption might occur, leading to processing issues and constant packet drop. [PR1243724](#)
- When switchover and zeroize are done in quick succession, zeroize will delete the databases,. If dfwd starts the signup processing after the zeroize, it will generate a core file as the database is not present. Zeroize should be done when the system is in stable state; that is, signups processing by daemons is completed.[PR1262385](#)
- On QFX5110 switches, an EVPN-VXLAN configuration using a custom-IRB MAC (same IP address, same MAC profile) might not work. As a workaround, we recommend you use a virtual gateway address. [PR1291406](#)
- Performing GRES on the EVPN-VXLAN topology with uRPF results in total packet loss. [PR1322217](#)
- BGP strongly recommends the configuration of local-address for each multihop iBGP/eBGP peer configuration. As a recommendation, local-address should be set to route-able lo0 address. Using a loopback address reduces dependency with interfaces. Note: Multihop is by default enabled for iBGP peers. [PR1323557](#)
- On a QFX5200 Virtual Chassis, traffic loss of 0.04 percent is seen with a Routing Engine switchover for the GRE tunnel scale test. [PR1323884](#)
- In a scaled setup, when the host table is full and the host entries are installed in LPM table, OSPF sessions might take more time to come up. [PR1358289](#)
- L3-GW is not supported on QFX5110 with SP style of configuration in Junos OS Release 17.3R3. [PR1363708](#)

Software Installation and Upgrade

- On QFX10K series, password recovery does not work, the commit fails when recovering a password. [PR1368986](#)

SEE ALSO

New and Changed Features	 255
Changes in Behavior and Syntax	 272
Known Behavior	 276
Resolved Issues	 287
Documentation Updates	 299
Migration, Upgrade, and Downgrade Instructions	 300
Product Compatibility	 313

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 17.3R3](#) | [287](#)
- [Resolved Issues: 17.3R2](#) | [293](#)
- [Resolved Issues: 17.3R1](#) | [297](#)

This section lists the issues fixed in the Junos OS main release and the maintenance releases.

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

Resolved Issues: 17.3R3

General Routing

- On QFX10000 switches, when using the auto-RP, the Protocol Independent Multicast egress interface disappears after a few minutes. [PR1063448](#)
- The LAG interface input bytes counter continuously decreases when no packets come in. [PR1266062](#)

- DHCP client is not working on the replacement build release. [PR1296774](#)
- SFP management Ethernet port C0 might not come up. [PR1298876](#)
- Traffic loss might be seen if sending traffic through the 40G interface. [PR1309613](#)
- One aggregated Ethernet member does not send out sFlow sample packets. [PR1311559](#)
- Traffic loss is observed while performing NSSU. [PR1311977](#)
- Certain IGMP join packets cannot be processed correctly at a high rate. [PR1314382](#)
- Transit traffic over GRE tunnel might hit the CPU and trigger a DDoS violation on the L3 next hop. [PR1315773](#)
- On a Layer 2 next-generation switch platform (EX4300/EX4600/EX9200QFX5100/QFX10000), the l2cpd process might drop core files repeatedly if an interface is connected to a VoIP product with LLDP and LLDP-MED, enabled. [PR1317114](#)
- Packets such as TDLS without an IP header are looped between the virtual gateways. [PR1318382](#)
- The optic interface still transmits power after it has been administratively shut down. [PR1318997](#)
- The packet might be dropped between 4-60 seconds when the master Routing Engine is rebooted in a Virtual Chassis. [PR1319146](#)
- The chassis MIB SNMP OIDs for VC-B member chassis are not available after an MX-VC ISSU. [PR1320370](#)
- The MAC address is stuck with "DR" flag on the spine node even though packets are received on an interface from the source MAC. [PR1320724](#)
- On the QFX10016 EVPN-VXLAN scaled testbed, it takes up to 3 minutes for traffic to converge during a configuration. [PR1323042](#)
- The openflow session cannot be established correctly with **controller** and **interfaces** options configured on QFX5100 Series switches. [PR1323273](#)
- You need to upgrade to new firmware versions for jfirmware package to resolve issues for 100G-PSM4 and 100G-AOC. [PR1323321](#)
- For EVPN of Type-5, the unicast traffic is getting dropped on the backup forwarder. [PR1323907](#)
- The next hop of _all_ces__ flood details might go missing. [PR1324739](#)
- VLAN or VLAN bridge might not be added or deleted if there is an IFBD HW token limit exhaustion. [PR1325217](#)
- The ARP request packets might not be flooded on the QFX5110. [PR1326022](#)
- The major alarm about **Fan & PSU Airflow direction mismatch** might be seen by removing the management cable. [PR1327561](#)
- Deleting one VXLAN might cause traffic loop on another VXLAN in multi-homing EVPN/VXLAN scenario with Service Provider style interface. [PR1327978](#)

- On a QFX10002, a major alarm should be cleared once the chassis has more PEM units installed than the "minimum PEM" configuration. [PR1327999](#)
- The fan tray removal or insertion trap is not generated for the backup FPC. [PR1329031](#)
- CoS is wrongly applied on Packet Forwarding Engine leading to egress traffic drop. [PR1329141](#)
- The etherStatsCRCAlignErrors counters might disappear in the SNMP tree. [PR1329713](#)
- After commit, members of VC or VCF are split and some members might get disconnected. [PR1330132](#)
- After IP address move, the ARP table information is not in sync between the two spines. [PR1330663](#)
- The rpd process generates core files on the new backup Routing Engine at task_quit,task_terminate_timer_callback,task_timer_dispatch,task_scheduler after disabling NSR+GRES. [PR1330750](#)
- The **out of HMC range** and **HMC READ failed** error messages are seen. [PR1332251](#)
- Traffic does not pass through VCP ports after rebooting the VC members. [PR1332515](#)
- For EVPN-VXLAN, the designated forwarder drops multicast traffic. [PR1333069](#)
- The SIB LEDs on the fan tray are off after the replacement of the Fan Tray Controllers (FTC). [PR1334006](#)
- The DHCPv6 SOLICIT message is dropped. [PR1334680](#)
- The SNMP jnxBoxDescr OID returns a different value when upgrading to Junos OS Release 17.2. [PR1337798](#)
- The traffic coming from the remote VTEP PE might be dropped. [PR1338532](#)
- The analyzer status might be show as down when port mirroring is configured to mirror packets from an aggregated Ethernet member. [PR1338564](#)
- The VXLAN traffic might not be transmitted correctly with an IRB interface as an underlay interface of the VTEP tunnel. [PR1338586](#)
- The DDoS counters for OSPF might not increase. [PR1339364](#)
- The l2ald process generates core files at ../../../../src/junos/usr.sbin/l2ald/l2ald_vxlan_evpn.c:1603, when moving host between two multihomed interfaces. [PR1339543](#)
- Multicast traffic drop is seen if downstream IRB interfaces have snooping enabled. [PR1340003](#)
- Layer 3 traffic is not getting converged properly upon disabling the ECMP link between spine and leaf with EVPN-VXLAN configurations. [PR1343172](#)
- BPDU packets might get dropped and bpdud-block-on-edge might not work. [PR1343330](#)
- Broadcast frames might be modified with the ethertype 0x8850. [PR1343575](#)
- In an EVPN VXLAN with a flexible-tag mode deployment, 100G interface statistics do not get updated for ingress traffic. [PR1343746](#)
- The ARP reply packet auto generates the virtual gateway MAC in the Ethernet header. [PR1344990](#)

- QFX5100 - Fan RPM fluctuates when temperature sensor reaches its threshold. [PR1345181](#)
- CPU and Memory statistics not populating for backup switch in QFX5110 Virtual Chassis. [PR1346268](#)
- Incorrect inner VLAN tag is sent from QFX10K platform with Q-in-Q configured on the Layer 3 sub-interface. [PR1346371](#)
- Statistics process PFED might crash on an upgrade between certain releases. [PR1346925](#)
- QFX5100-48T 10G interface might be autonegotiated at 100 Mbps speed instead of 10 Gbps. [PR1347144](#)
- The IPFIX flow stats are incorrect in the exported record. [PR1347229](#)
- The part numbers and serial numbers are not displayed for any of the 10G optics/dac connected. [PR1347634](#)
- Traffic is discarded with destination MAC matching the virtual gateway MAC might be seen. [PR1348659](#)
- The pfed process is consuming 80 to 90 percent of CPU, running subscriber management on PPC based routers. [PR1351203](#)
- The GTP traffic might not be hashed correctly for the aggregated Ethernet interface. [PR1351518](#)
- The RPC output is not showing failure when running **request system software add** with software already staged. [PR1353466](#)
- The alarm errors might be seen during the bootup on QFX10000. [PR1354582](#)
- Untagged packets might not be forwarded through the trunk port. [PR1355338](#)
- On QFX5110 platforms, LX10 SFP needs to be reinserted after autonegotiation is enabled or disabled. [PR1355746](#)
- The VXLAN traffic might be lost in EVPN type 2 and type 5 scenario. [PR1355773](#)
- Spine switches might lose connectivity to the core network. [PR1357296](#)
- The IGMP membership report packets might not be forwarded over an interface on QFX10k. [PR1360137](#)
- The GTP traffic might not be hashed correctly for aggregated Ethernet interface. [PR1361379](#)
- The **clear services accounting statistics inline-jflow fpc-slot 0** command should be supported in QFX. [PR1362396](#)
- The proxy ip+mac advertisements are not advertised by spine when host is learned from remote Layer 2 GW and installed in arp table [PR1364591](#)
- On QFX5110, QFX5200, or QFX10000 switches, there is an issue with the root password recovery via console. [PR1365740](#)

EVPN

- On EVPN-VXLAN QFX10000, the jprds_dlu_alpha_add : 222 JPRDS_DLU_ALPHA KHT addition failed. [PR1258933](#)
- On a VXLAN-EVPN, there is IPv6 packet loss after a normal traffic run rate. [PR1267830](#)

- The sub interface from the same physical port does not work if configured under the same VXLAN VLAN. [PR1278761](#)
- When a VLAN uses an IRB interface as the routing interface, the vlan-id parameter must be set to "none" to ensure proper traffic routing. This issue is platform independent. [PR1287557](#)
- For JDISwitchingReg, a VXLAN traffic loss is observed after deleting and adding VLANs. [PR1318045](#)
- In Ethernet VPN (EVPN) or Virtual Extensible LAN (VXLAN), a Layer 3 gateway scenario with multihoming mode configured, the remote Address Resolution Protocol (ARP) entry might not be deleted correctly after deactivating/activating the aggregated Ethernet interface (AE interface with esi configured) or rebooting the device. It will cause traffic to be dropped. [PR1326691](#)
- A core link flap might result in an inconsistent global MAC count. [PR1328956](#)
- The partial multicast traffic might be dropped in an EVPN-VXLAN multihoming scenario with a non-default virtual switch or an EVPN routing-instance configured. [PR1334408](#)
- On QFX5100 EVPN-VXLAN, the leaf is forwarding traffic to an incorrect VTEP after a MAC move or vmotion. [PR1335431](#)
- The ARP entry might be deleted in redundant Layer 3 gateway EVPN-VXLAN scenario after IP address move happens. [PR1336185](#)
- Configuring encapsulate-inner-vlan on the partial VXLANs might cause traffic impact. [PR1337953](#)
- In an EVPN/VXLAN environment, BFD flaps cause VTEP flaps and cause a Packet Forwarding Engine crash. [PR1339084](#)
- The rpd process generates unreproducible core files with scaling EVPN-VXLAN configuration on QFX10K platform. [PR1339979](#)
- The rpd process might generate core files on deleting the default-switch in an EVPN-VXLAN environment. [PR1342351](#)
- The traffic might get dropped as the core is down. [PR1343515](#)
- Traffic might be lost on Layer 2 and Layer 3 spine node in multi home EVPN scenario. [PR1355165](#)
- Increased risk of routing crash with temporary impact on traffic on QFX10000 or QFX5100 nodes with certain configuration changes or clearing Layer 2 or Layer 3 learning information a high-scale EVPN-VXLAN configuration environment [PR1365257](#)
- The VTEPs MAC address is not learnt in the Ethernet switching table. [PR1371995](#)

High Availability (HA) and Resiliency

- When **igmp-snooping** and **bpdu-block-on-edge** are enabled, the IP protocol multicast traffic sourced by the kernel (such as, OSPF and VRRP) gets dropped in the Packet Forwarding Engine level. [PR1301773](#)

Interfaces and Chassis

- Multicast data packets are looping in MC-LAG. [PR1281646](#)

- On QFX5K and EX4600 platforms, if ICL is configured on single interface (without LAG) and remote MCAE is down, and both MCLAG peers are rebooted, sometimes packets might drop on ICL of MCLAG peer where MCAE is up. [PR1345316](#)
- If CVLANs range is 16, it might not pass traffic in a Q-in-Q scenario. [PR1345994](#)

Layer 2 Features

- The NLB heartbeat packets might be dropped on QFX10000 or PTX Series. [PR1322183](#)
- The ARP entry might be learned on STP blocking ports. [PR1324245](#)
- MAC learning might fail for a device on an extended port of a satellite device after a MAC move in a Junos Fusion scenario. [PR1324579](#)
- The DHCP discover packets might be looped in an MC-LAG and a DHCP-relay scenario. [PR1325425](#)
- On a QFX5100 with multiple logical units configured on an interface, the input VLAN map point of presence (POP) is not removing the outer VLAN tag when Q-in-Q and VXLAN are involved. [PR1331722](#)
- Push is not working for VXLAN local switching for Q-in-Q. [PR1332346](#)
- The interface with flexible VLAN tagging and family Ethernet switching does not work on QFX10000. [PR1337311](#)
- Traffic stops passing through the EVPN interface configured with encapsulation Ethernet bridge, unit 0; after code upgrade from Junos OS Release 15.1X53-D65 to Junos OS Release 17.3R2. [PR1344874](#)

Layer 2 Ethernet Services

- The jdncpd process generates core files after making DHCP configuration changes. [PR1324800](#)

MPLS

- On QFX5100, unified ISSU is not supported with MPLS configuration. [PR1264786](#)
- Traffic drops during NSR switchover for RSVP P2MP provider tunnels used by MVPN. [PR1293014](#)
- MPLS forwarding might not happen properly for some LSPs. [PR1319379](#)
- The rpd process might crash on the backup Routing Engine due to memory exhaustion. [PR1328974](#)
- The hot standby for I2circuit does not work on a QFX5100. [PR1329720](#)
- RSVP sessions goes down for ingress LSPs with no-cspf enabled. [PR1339916](#)
- The NO-propagate-TTL acts on MPLS swap operation. [PR1366804](#)

Platform and Infrastructure

- Directories and files under `/var/db/scripts` lose execution permission or directory 'jet' is missing under `/var/db/scripts` file causing the following error: **Invalid directory: No such file or directory** error during commit [PR1328570](#)
- While downgrading a Junos OS software from a later release, the router goes into amnesiac state. [PR1341650](#)

- The ARP might not update and packets might get dropped at the Routing Engine. [PR1348029](#)

Routing Protocols

- An mcsnoopd core file is observed at (enable_slip_detector=true, no_exit=true) at `../../../../src/junos/lib/libtask/base/task_scheduler.c:275`. [PR1305239](#)
- Diffserv bits/ToS bits are not getting copied from the inner IP header to the GRE header. [PR1313311](#)
- Some of the IPv4 multicast routes in the Packet Forwarding Engine might fail to install and update. [PR1320723](#)
- On a QFX5100, consistent hashing is not getting programmed. [PR1322299](#)
- The IS-IS Layer 2 hello packets are dropped when they come from a Brocade device. [PR1325436](#)
- The loopbacked IRB interface is not accessible to the remote network. [PR1333019](#)
- The dcpfe process crash is seen in route leak scenario on a QFX10000. [PR1334714](#)
- The reverse path forwarding (RPF) check policy does not work as expected. [PR1336909](#)
- Ping fails if MTU is different on the interfaces. [PR1345495](#)
- Parity error in Layer 3 IPv4 table. [PR1364657](#)

Resolved Issues: 17.3R2

Hardware

- The 1G copper module interface shows "Link-mode: Half-duplex" on QFX10000 line platforms. [PR1286709](#)
- ULC-60S-6Q LC on QFX10008: The port becomes unusable after inserting a third-party SFP-T optic. [PR1294394](#)

Class of Service (CoS)

- On EX4300, EX4600, or QFX5100, traffic might be dropped when there is more than one forwarding class under "forwarding-class-sets". [PR1255077](#)

EVPNs

- Next-hop installation error messages are seen on QFX10000 line switches. [PR1258930](#)
- QFX10002 VXLAN with MPLS underlay seen traffic loss at RSVP egress [PR1289666](#)
- On QFX5100 switches with EVPN-VXLAN deployed, broadcast and multicast traffic might not be sent to other switches through VTEP interfaces. [PR1293163](#)
- On QFX10000 switches with EVPN deployed, packet corruption is seen with Packet Forward Engine trap code (129) `egp.v4_chksum` when sending L3 inter-VNI traffic with the underlay vlan-tagging inet interface. [PR1295491](#)

- df-election-type preference statements in the [show interfaces esi] hierarchy level are not supported on QFX10000 running Junos OS Release 17.3R1. [PR1300093](#)
- The dynamic routing protocols might not work correctly over the IRB interface in an EVPN-VXLAN scenario with ECMP. [PR1301521](#)
- RPD crash on loading EVPN configurations in qfx10002-72q. [PR1305440](#)
- EVPN Proxy ARP might work properly. [PR1312672](#)

Interfaces and Chassis

- Multicast data packets are looping in MC-LAG. [PR1281646](#)
- ARP reply drop in MC-LAG scenario. [PR1282349](#)
- On QFX5100 switches, an AE interface might flap upon commit if an explicit speed is configured on an AE member interface. [PR1284495](#)
- Traffic might not be received on a 1-Gigabit Ethernet interface if autonegotiation is disabled and speed/duplex is configured on both the QFX Series switch and the peer host. [PR1292275](#)
- The 40-Gigabit Ethernet interface might not come up if a specific vendor's DAC cable is used. [PR1296011](#)
- On QFX Series platforms, the connectivity of IPv4 might be lost if the Logical interface (IFL) gl2d-property (eth) bit is set to 0. [PR1297594](#)
- On QFX Series platforms with ZTP environment, the DHCP clients are not getting an IP address with /31 subnet in server configuration. [PR1298234](#)
- The dcpfe process might crash and restart on MC-LAG active and standby nodes when there is ARP/NDP next-hop change. [PR1299112](#)
- Disabled 10-Gigabit Ethernet interfaces might stay up on QFX10000 line switches. [PR1300775](#)
- QFX10008/10016: Commit error is seen when configured with mixed speed. [PR1301923](#)
- On QFX5100/5110/5200 devices, IGMP snooping entries are not learnt on MCLAG peer. [PR1302620](#)
- QSFP+4x10G-IR channelized interface down between QFX5200 and PTX5000 [PR1307400](#)
- Upgrading to 16.1R5 without "redundancy-group-id-list" statement prior in ICCP leads to commit failure during bootup. [PR1311009](#)
- Core link flap might result in an inconsistent global MAC count. [PR1328956](#)

Layer 2 Features

- Feature swap-swap might not work as expected in a Q-in-Q scenario. [PR1297772](#)
- Device transmits packets that exceed the interface MTU. [PR1306724](#)
- NLB heartbeat packets might be dropped on QFX10000/PTX. [PR1322183](#)
- The DHCP Discover packets might be looped in MC-LAG and DHCP-Relay scenario. [PR1325425](#)

Layer 3 Features

- QFX5110-48S: L3 VPN traffic is dropped for some instances when EVPN-VXLAN configuration is removed and reapplied. [PR1307590](#)

Management

- QFX5110-48S: digital optical monitoring statistics cannot be received through the CLI in Junos OS Releases 15.1X53 through 17.x. [PR1305506](#)

MPLS

- QFX5100: ISSU is not supported with MPLS configuration. [PR1264786](#)
- 17.3: U8: QFX10008 is dropping the egress MPLS traffic, if the egress interface is an IRB with access L2 AE interface. [PR1279827](#)
- DHCP clients cannot get IP addresses over BGP-L3VPN. [PR1303442](#)
- LSP stop transferring/passing traffic after MPLS route is changed. [PR1309058](#)
- MPLS forwarding might not happen properly for some LSPs. [PR1319379](#)

Network Management and Monitoring

- UFT for non-local member is not shown in the CLI. [PR1243758](#)
- MACsec issue: "show security macsec statistics" command does not show expected results. [PR1283544](#)
- SNMP process is not running on QFX Series switches with incorrect source addresses. [PR1285198](#)

Platform and Infrastructure

- Traffic loss might be observed for about 10 seconds if master member FPC reboots. [PR1283702](#)
- QFX10002 and QFX10008: BFD sessions over IRB interfaces with Junos OS Releases 17.1R1, 17.1R2, 17.2R1, and 17.3R1 are centralized. [PR1284743](#)
- The dexp process might crash after committing **set system commit delta-export**. [PR1284788](#)
- Storm-control flags are not set after a Routing Engine switchover. [PR1290246](#)
- OSPFv3 authentication using IPsec SA does not work if you are using IPsec to authenticate OSPFv3 neighbors on some QFX Series platforms. [PR1301428](#)
- The sflow records are missing "extendedType ROUTER" fields as well as an outbound interface for traffic that is using BGP multipath. [PR1303236](#)
- The FPC memory might be exhausted with SHEAF leak messages seen in the syslog. [PR1311949](#)
- JDISwitchingReg : Traffic loss is observed while performing NSSU. [PR1311977](#)
- CPU utilization is around 50% without any configuration. [PR1312520](#)
- On QFX5200 Virtual Chassis, 100G port VCP not supported. [PR1314922](#)

- Transit traffic over GRE tunnel might hit the CPU and trigger a DDoS violation on the L3 next hop. [PR1315773](#)
- On an L2 next-generation switch platform (EX4300/EX4600/EX9200/QFX5100/QFX10000), l2cpd might drop core files repeatedly if an interface is connected to a VoIP product with LLDP and LLDP-MED enabled. [PR1317114](#)
- Port speed is still showing 100G instead of 50G because the physical interface (IFD) has been channelized to 50G. [PR1319884](#)
- FPCs go offline due to the error **CHASSISD_IPC_CONNECTION_DROPPED: Dropped IPC connection for FPC**. [PR1321198](#)
- EVPN Type 5: Unicast traffic is getting dropped on the backup forwarder. [PR1323907](#)
- QFX5100/EX4600/ACX5k : Major Alarm 'Fan & PSU Airflow direction mismatch' by removing management cable. [PR1327561](#)
- QFX10002: Major alarm should be cleared once the chassis has more PEM units installed than the "minimum PEM" configuration. [PR1327999](#)

Port Security

- Proxy-ARP and ARP suppression are not yet supported for the QFX10000 line. [PR1293707](#)

Routing Policy and Firewall Filters

- The rpd might crash if **vrf-target auto** is configured under routing-instance. [PR1301721](#)

Routing Protocols

- OVSDB and Openflow have some limitations on QFX5110, QFX5200, QFX10002, QFX10008, and QFX10016 switches running Junos OS Releases 17.1R1, 17.1R2, and 17.2R1. [PR1288227](#)
- FBF with next-ip/next-ip6/next-interface is not working. [PR1289642](#)
- Remotely received traffic is not flooded to AC on FPC 1 when FPC 0 was offlined. [PR1290500](#)
- IPv6 multicast traffic drop occurs in PIM SSM scenario. [PR1292519](#)
- On QFX5100, the fxpc process generates a core file. [PR1294033](#)
- The dcpfe process might crash after a period of idle time on QFX10000 switches. [PR1294055](#)
- If MPLS LSP self-ping is enabled (self-ping is enabled by default), the kernel might panic with an error message **Fatal trap 12: page fault while in kernel mode.** [PR1303798](#)
- Observed **mcsnoopd** core file at `__raise,abort,__task_quit,__task_quit,task_terminate_timer_callback,task_timer_dispatch,task_scheduler_internal (enable_slip_detector=true, no_exit=true)` at `../../../../src/junos/lib/libtask/base/task_scheduler.c:275`. [PR1305239](#)
- Packets drop is seen when programming for GRE traffic. [PR1308438](#)

Software Installation and Upgrade

- After upgrading the QFX5100-96s-8q to Junos OS Release 16.1R4 from Junos OS Release 15.1R4, showing commit warning '/boot/ffp.cookie+'. [PR1283917](#)

Virtual Chassis

- QFX5100 TVP: Not able to load TVP image on top of a non-TVP 5100 image while adding a QFX5100 switch to the Virtual Chassis. [PR1248145](#)
- QFX5200: New apply group not applying to the Virtual Chassis after a reboot. [PR1305520](#)
- QFX-VC: Sometimes seeing that Multicast packets received 2x 3x times than expected. [PR1306239](#)
- QFX5110 VC/VCF: VC members reboot before all members have image installed. [PR1309103](#)
- Some log messages are seen on the QFX5110 platform when plugging in an SFP-SX. [PR1311279](#)

Resolved Issues: 17.3R1

General Routing

- On QFX10000 line switches, sFlow monitoring technology output might display a negative number of samples after a long run. As a workaround, issue the **clear sflow collector** command to show or reset the count. [PR1244080](#)
- VLAN association is not being updated in the Ethernet switching table when the device is configured in single supplicant mode. [PR1283880](#)
- Hostname synchronization from Junos VM instance to Linux Host in TVP Platforms (QFX). [PR1283710](#)

Interfaces and Chassis

- Interfaces randomly do not come up after a line card restart. [PR1262839](#)
- On QFX5100 switches, a 40G interface may keep flapping when a 5M DAC cable is inserted. [PR1273861](#)
- On QFX10000 switches, there may be an ot- link flap whenever there is an optics TCA alarm, however there is no loss of signal and no traffic loss observed. [PR1279351](#)
- FEC disabled by default on 100G-LR optics for QFX5200 switches. [PR1286389](#)

Layer 2 Features

- All the XML duplications and unformatted output are addressed. For Example, histogram was just declared as a element inside pfkey container, with this change a new container is defined for histogram. [PR1271648](#)

Port Security

- On QFX10000 switches, MACsec sessions are not coming up on a Layer 3 sub-interface. [PR1282995](#)

Routing Protocols

- When static Link protection mode configured back up state as down, primary port is going to down state instead of secondary port while secondary is at up state. [PR1276156](#)
- UDP traffic with destination port 520 and 521 is discarded on QFX5110 switches after a Junos OS upgrade. [PR1287271](#)
- In a data center environment with EVPN/VXLAN and proxy MAC plus IP advertisement enabled on a Layer 3 gateway, the state for some MACs may be lost during MAC moves. [PR1291118](#)

System Management

- Multicast Listener Discovery (MLD) messages are seen continuously on QFX switches if the management ports are connected through a network. [PR1277618](#)
- Analytics json data format reporting incorrect value for 'rxbps' counter. [PR1285434](#)

VXLAN

- Two new CLI commands are added: **set forwarding-options vxlan-routing next-hop *number*** ; **set forwarding-options vxlan-routing interface-num *number***. These commands are applicable only for QFX5110 switches. [PR1259323](#)

SEE ALSO

[New and Changed Features | 255](#)

[Changes in Behavior and Syntax | 272](#)

[Known Behavior | 276](#)

[Known Issues | 281](#)

[Documentation Updates | 299](#)

[Migration, Upgrade, and Downgrade Instructions | 300](#)

[Product Compatibility | 313](#)

Documentation Updates

IN THIS SECTION

- [Traffic Management User Guide for the QFX Series | 299](#)

This section lists the errata and changes in Junos OS Release 17.3R3 for the QFX Series switches documentation.

Traffic Management User Guide for the QFX Series

- **Consolidation of the Traffic Management User Guide for QFX Series and EX4600 Switches (QFX Series)**—Starting in Junos OS Release 17.3R1, the following three traffic management guides are consolidated into one user guide:
 - Traffic Management User Guide for QFX Series
 - Traffic Management User Guide for QFX 10000 Series
 - Traffic Management User Guide for EX4600 Switches

[See [Traffic Management User Guide for QFX Series and EX4600 Switches.](#)]

SEE ALSO

[New and Changed Features | 255](#)

[Changes in Behavior and Syntax | 272](#)

[Known Behavior | 276](#)

[Known Issues | 281](#)

[Resolved Issues | 287](#)

[Migration, Upgrade, and Downgrade Instructions | 300](#)

[Product Compatibility | 313](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrading Software on QFX Series Switches | 300
- Installing the Software on QFX10002 Switches | 303
- 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 | 303
- Installing the Software on QFX10008 and QFX10016 Switches | 305
- Performing a Unified ISSU | 309
- Preparing the Switch for Software Installation | 310
- Upgrading the Software Using Unified ISSU | 310

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

Upgrading Software on QFX Series Switches

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

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

1. In a browser, go to <https://support.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 **17.3** 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 17.3 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-10-f-x86-64-17.3
-R3.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 17.3 **jinstall** package, you can issue the **request system software rollback** command to return to the previously installed software.

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 17.3R2.

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

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

For example:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-f-x86-64-17.3  
-R3.n-secure-signed.tgz reboot 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-x86-64-17.3  
-R3.n-secure-signed.tgz reboot 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://support.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://support.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-x86-64-17.3  
-R3.n-secure-signed.tgz reboot
```

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-x86-64-17.3
-R3.n-secure-signed.tgz reboot
```

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 for upgrading to Junos OS Release 17.3R2 from 17.1R1 or later. Upgrading to 17.3R2 from releases prior to 17.1R1 is not supported. For example, upgrading from Junos OS Release 14.1X53 to 17.3R2 is not supported.

Perform the following tasks:

- [Preparing the Switch for Software Installation on page 310](#)
- [Upgrading the Software Using Unified ISSU on page 310](#)

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-x86-64-17.3-R3.n-secure-signed.tgz` **reboot**.

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-x86-64-17.3
-R3.n-secure-signed.tgz reboot ...
Install jinstall-host-qfx-5-f-x86-64-17.3
-R3.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.

SEE ALSO

New and Changed Features 255
Changes in Behavior and Syntax 272
Known Behavior 276
Known Issues 281
Resolved Issues 287
Documentation Updates 299
Product Compatibility 313

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 313

Hardware Compatibility

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.

To determine the features supported on QFX Series switches in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://pathfinder.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

New and Changed Features 255
Changes in Behavior and Syntax 272
Known Behavior 276

[Known Issues | 281](#)

[Resolved Issues | 287](#)

[Documentation Updates | 299](#)

[Migration, Upgrade, and Downgrade Instructions | 300](#)

Junos OS Release Notes for SRX Series

IN THIS SECTION

- [New and Changed Features | 314](#)
- [Resolved Issues | 320](#)
- [Migration, Upgrade, and Downgrade Instructions | 324](#)
- [Product Compatibility | 327](#)

Junos OS Release 17.3R3 and later Junos OS 17.3 releases are not supported for SRX Series devices and vSRX instances. Junos OS Release 17.3R2 is the last release for the Junos OS 17.3 release train that is supported for SRX Series devices and vSRX instances.

To find the release notes for Junos OS Release 17.3 for releases that are supported for SRX Series devices, go to the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

New and Changed Features

This section describes the new features and enhancements to existing features in the Junos OS main release and the maintenance releases for the SRX Series devices.

Release 17.3R2 New and Changed Features

There are no new features in Junos OS Release 17.3R2 for the SRX Series devices.

Release 17.3R1 New and Changed Features

IN THIS SECTION

- [Flow and Processing | 315](#)
- [IDP | 316](#)
- [Interfaces and Chassis | 317](#)
- [Junos OS XML API and Scripting | 317](#)
- [Layer 2 Features | 317](#)
- [Management | 318](#)
- [Network Security | 318](#)
- [Software Installation and Upgrade | 318](#)
- [User Interface and Configuration | 319](#)

Junos OS Release 17.3R1 supports the following Juniper Networks security platforms: vSRX, SRX300/320, SRX340/345, SRX550HM, SRX1500, SRX4100/4200, SRX5400, SRX5600, and SRX5800. Most security features in this release were previously delivered in Junos OS for SRX Series “X” releases from 12.1X44 through 15.1X49-D75. Security features delivered in Junos OS for SRX Series “X” releases after 15.1X49-D75 are not available in 17.3R1.

New features for security platforms in Junos OS Release 17.3R1 include:

Flow and Processing

- **TCP out-of-state packet drop logging (SRX Series)**—Starting in Junos OS Release 17.3R1, SRX Series devices support logging of unsynchronized TCP out-of-state packets that are dropped by the flow module.

Within any packet-switched network, when demand exceeds available capacity, the packets are queued up to hold the excess packets until the queue fills, and then the packets are dropped. When TCP operates across such a network, it takes any corrective actions to maintain error-free end-to-end communications.

This feature enables packet recovery by logging the out-of-sync packets for error-free communication, and avoids database servers going out of sync.

TCP packet drop logging occurs when:

- TCP packets that trigger session creation are not synchronized.
- TCP three-way handshake in flow fails.

- TCP sequence check in flow fails.
- TCP SYN packets are received in TCP FIN state.

The unsynchronized TCP out-of-state packet drop log is a packet-based log, not a session-based log.

NOTE: TCP packets that are dropped by TCP-proxy and IDP are not logged.

[See [TCP Out-of-State Packet Drop Logging Overview](#).]

IDP

- **IPS signature package update (SRX Series and vSRX instances)**—Starting with Junos OS Release 17.3, when you upgrade from Junos OS Release 12.3X48 or 15.1X49 to Junos OS Release 17.3 or downgrade from Junos OS Release 17.3 to Junos OS Release 12.3X48 or 15.1X49, you must update the IPS signature package to avoid any IDP configuration commit failures. Update the IPS signature package by:
 - Downloading the IPS signature package.
 - Installing the IPS signature package update when the download completes.

NOTE: When you upgrade from Junos OS Release 15.1X49 to Junos OS Release 17.3, the following warning message is displayed:

```
WARNING: A full install of the security package is required after reboot.
WARNING: Please perform a full update of the security package using
WARNING:      "request security idp security-package download full-update"
WARNING: followed by
WARNING:      "request security idp security-package install"
```

[See [Downloading and Installing the IPS Signature Package from an Older Junos OS Release Version to Newer Junos OS Release Version.](#)]

Interfaces and Chassis

- **Promiscuous mode support (SRX5400, SRX5600, SRX5800)**—Promiscuous mode function is supported on the SRX5000 line MPC (SRX5K-MPC) on 1-Gigabit, 10-Gigabit, 40-Gigabit, and 100-Gigabit Ethernet interfaces on the MICs.

By default, an interface enables MAC filtering. You can configure promiscuous mode on the interface to disable MAC filtering. When you delete the promiscuous mode configuration, the interface will perform MAC filtering again. You can change the MAC address of the interface even when the interface is operating in promiscuous mode. When the interface is operating in normal mode again, the MAC filtering function on MPC uses the new MAC address to filter packets.

[See [Understanding Promiscuous Mode on Ethernet Interfaces.](#)]

Junos OS XML API and Scripting

- **Support for Python language for commit, event, op, and SNMP scripts (SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances)**—Starting in Junos OS Release 17.3R1, you can author commit, event, op, and SNMP scripts in Python on devices that include the Python extensions package in the software image. Creating automation scripts in Python enables you to take advantage of Python features and libraries as well as leverage Junos PyEZ APIs supported in Junos PyEZ Release 1.3.1 and earlier releases to perform operational and configuration tasks on devices running Junos OS. To enable execution of Python automation scripts, which must be owned by either root or a user in the Junos OS **super-user** login class, configure the **language python** statement at the **[edit system scripts]** hierarchy level, and configure the filename for the Python script under the hierarchy level appropriate to that script type. Supported Python versions include Python 2.7.

[See [Understanding Python Automation Scripts for Devices Running Junos OS.](#)]

Layer 2 Features

- **LACP support in Layer 2 transparent mode (SRX5400, SRX5600, and SRX5800)**—Starting with Junos OS Release 17.3R1, LACP is supported in Layer 2 transparent mode in addition to existing support in Layer 3 mode.

When the SRX Series device uses LACP to bundle the member links, it creates high-speed connections, also known as *fat pipe*, with peer systems. Bandwidth can be increased by adding member links. Increased bandwidth is especially important for redundant Ethernet (reth) and aggregated Ethernet (ae) interfaces. LACP also provides automatic determination, configuration, and monitoring member links.

LACP is compatible with other peers that run the 802.3ad LACP protocol. It automatically binds member links without manually configuring the LAG, thereby avoiding errors.

NOTE: Tentative sessions are created for all interfaces in a particular VLAN. If there is plenty of one-way traffic, numerous tentative sessions are created. When sessions reach the maximum limit, vector fails and packet loss might be seen.

Management

- **Support for adding non-native YANG modules to the Junos OS schema (SRX345, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances)**—Starting in Junos OS Release 17.3R1, you can load custom YANG models on devices running Junos OS to add data models that are not natively supported by Junos OS but can be supported by translation. Doing this enables you to extend the configuration hierarchies and operational commands with data models that are customized for your operations. The ability to add data models to a device is also beneficial when you want to create device-agnostic and vendor-neutral data models that enable the same configuration or RPC to be used on different devices from one or more vendors. You can load custom YANG modules by using the **request system yang add** operational command.

[See [Understanding the Management of Non-Native YANG Modules on Devices Running Junos OS](#).]

Network Security

- **Maximum number of security policies increased (SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 17.3R1, the maximum number of security policies for SRX5400, SRX5600, and SRX5800 devices has increased from 80,000 to 100,000.

[See [Best Practices for Defining Policies on SRX Series Devices](#).]

Software Installation and Upgrade

- **Support for FreeBSD version 10 for Junos OS (SRX5800, SRX5600, SRX5400)**—Starting with Junos OS Release 17.3R1, on the SRX5000 line of devices, FreeBSD version 10 is the underlying operating system for Junos OS. Junos OS with upgraded FreeBSD is based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. The newer FreeBSD kernel base provides Junos OS with sophisticated processing, efficiency, and security.

NOTE: On SRX5000 line of devices, use **no-validate** flag at the **request system software add <filename> no-validate** command to upgrade or downgrade between Junos OS Release 17.3 and the previous releases.

NOTE: Along with the upgraded FreeBSD, the System Snapshot feature has been enhanced on the SRX5000 line of devices. For more details, see [Junos OS with Upgraded FreeBSD](#)

[See [Understanding Junos OS with Upgraded FreeBSD](#).]

User Interface and Configuration

- **Support for configuring the ephemeral database using the NETCONF and Junos XML protocols (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances)**—Starting in Junos OS Release 17.3R1, NETCONF and Junos XML protocol client applications can configure the ephemeral configuration database, which is an alternate configuration database that enables multiple clients to simultaneously load and commit configuration changes on a device running Junos OS and with significantly greater throughput than when committing data to the candidate configuration database. Junos OS provides a default instance and up to eight user-defined instances of the ephemeral configuration database. The device's active configuration is a merged view of the committed configuration database and the configuration data in all instances of the ephemeral configuration database. Ephemeral configuration data is volatile and is deleted upon rebooting the device.

[See [Understanding the Ephemeral Configuration Database](#).]

SEE ALSO

[Resolved Issues](#) | [320](#)

[Migration, Upgrade, and Downgrade Instructions](#) | [324](#)

[Product Compatibility](#) | [327](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 17.3R2 | 320](#)
- [Resolved Issues: 17.3R1 | 322](#)

This section lists the issues fixed in the Junos OS main release and the maintenance releases.

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

Resolved Issues: 17.3R2

IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 321](#)
- [Authentication and Access Control | 321](#)
- [Chassis Clustering | 321](#)
- [CoS | 321](#)
- [Ethernet Switching | 321](#)
- [Flow-Based and Packet-Based Processing | 321](#)
- [J-Web | 321](#)
- [Network Address Translation \(NAT\) | 321](#)
- [Network Management and Monitoring | 321](#)
- [Platform and Infrastructure | 322](#)

Application Layer Gateways (ALGs)

- The pfed process crashes and generates core files. [PR1292992](#)

Authentication and Access Control

- SRX Series device assigns IP address 0.0.0.0 to xauth clients. [PR1315999](#)

Chassis Clustering

- The SRX1500 stops forwarding traffic randomly. [PR1277435](#)
- Duplicate RFSP IE drops the GTP packet. [PR1284311](#)
- After software upgrade, the cluster goes to short split-brain when rebooting RGO secondary, and multiple errors and issues are seen. [PR1288819](#)
- ISSU can be unsuccessful if control-link-recovery is configured. [PR1303948](#)

CoS

- On SRX1500 devices, CoS scheduler and shaping do not work on IRB interface. [PR1292187](#)

Ethernet Switching

- Ping to VRRP(VIP) address failed when VRRP on vlan-tagging. It only affects IOC2 and IOC3 cards in SRX5000 line devices. [PR1293808](#)

Flow-Based and Packet-Based Processing

- ECMP does not work for traffic with ECN enabled and with IPv6. [PR1265576](#)
- On SRX1500 devices, core files are generated when J-Flow is enabled. [PR1271466](#)
- More CPU threshold warnings are seen than in the previous releases. [PR1291506](#)
- SCTP association capacity cannot reach up to 20K. [PR1299186](#)
- The name daemon (named) might crash if SRX Series device is configured for dns-proxy. [PR1307435](#)

J-Web

- J-Web removes backslash character on source identity object when committing changes. [PR1304608](#)

Network Address Translation (NAT)

- The **show security zones detail** command causes memory leak. [PR1269525](#)

Network Management and Monitoring

- The mib2d process might crash when polling the OID ifStackStatus.0 after an a logical interface (IFL) of lo0 is deleted. [PR1286351](#)
- The **show arp no-resolve interface X** command for non-existent interface X is showing all unrelated static ARP entries. [PR1299619](#)

Platform and Infrastructure

- SRX Series device does not process traffic due to an IPv6 NA packets burst. [PR1293673](#)

Resolved Issues: 17.3R1

IN THIS SECTION

- [Interfaces and Chassis | 323](#)
- [Layer 2 Ethernet Services | 323](#)
- [Platform and Infrastructure | 323](#)
- [Routing Policy and Firewall Filters | 323](#)
- [Unified Threat Management \(UTM\) | 323](#)
- [VPNs | 323](#)

Interfaces and Chassis

- On SRX1500, if Junos OS Release 15.1X49-D70 or later is installed and you have a single PEM in slot 0, you will see an alarm saying PEM 1 is not present. [PR1265795](#)

Layer 2 Ethernet Services

- On SRX1500 devices, when configuring the devices to switching mode, an IRB interface located in a custom routing-instance is not reachable. [PR1234000](#)

Platform and Infrastructure

- On SRX Series devices in a chassis cluster, if sampling is used, the flowd process fails and core files are seen on both the nodes, when the route is updated through dynamic protocols such as BGP. [PR1249254](#)

Routing Policy and Firewall Filters

- Starting in Junos OS Release 15.1X49-D100, a new default application, application junos-smtps, has been added for secured e-mail traffic using port 587 or 465. To view the new default policy, use the **show configuration groups junos-defaults applications** command. [PR1273725](#)

Unified Threat Management (UTM)

- Some traffic from web-cam contain non-standard HTTP boundary format will cause SRX Series UTM/SAV to hold traffic/mbuf and later causes failover. [PR1283806](#)

VPNs

- On SRX5400, SRX5600, and SRX5800 devices, the st0 interface global counter statistics do not increment and remain zero, although traffic passes through the tunnel sub-interfaces such as st0.0 and st0.1. [PR1171958](#)

SEE ALSO

New and Changed Features 314
Known Issues
Documentation Updates
Migration, Upgrade, and Downgrade Instructions 324

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Scripts for Address Book Configuration | 324](#)

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.

Upgrade and Downgrade Scripts for Address Book Configuration

IN THIS SECTION

- [About Upgrade and Downgrade Scripts | 324](#)
- [Running Upgrade and Downgrade Scripts | 326](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 327](#)

Beginning with Junos OS Release 12.1, you can configure address books under the **[security]** hierarchy and attach security zones to them (zone-attached configuration). In Junos OS Release 11.1 and earlier, address books were defined under the **[security zones]** hierarchy (zone-defined configuration).

You can either define all address books under the **[security]** hierarchy in a zone-attached configuration format or under the **[security zones]** hierarchy in a zone-defined configuration format; the CLI displays an error and fails to commit the configuration if you configure both configuration formats on one system.

Juniper Networks provides Junos operation scripts that allow you to work in either of the address book configuration formats (see [Figure 1 on page 326](#)).

About Upgrade and Downgrade Scripts

After downloading Junos OS Release 12.1, you have the following options for configuring the address book feature:

- **Use the default address book configuration**—You can configure address books using the zone-defined configuration format, which is available by default. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

- **Use the upgrade script**—You can run the upgrade script available on the Juniper Networks support site to configure address books using the new zone-attached configuration format. When upgrading, the system uses the zone names to create address books. For example, addresses in the trust zone are created in an address book named **trust-address-book** and are attached to the trust zone. IP prefixes used in NAT rules remain unaffected.

After upgrading to the zone-attached address book configuration:

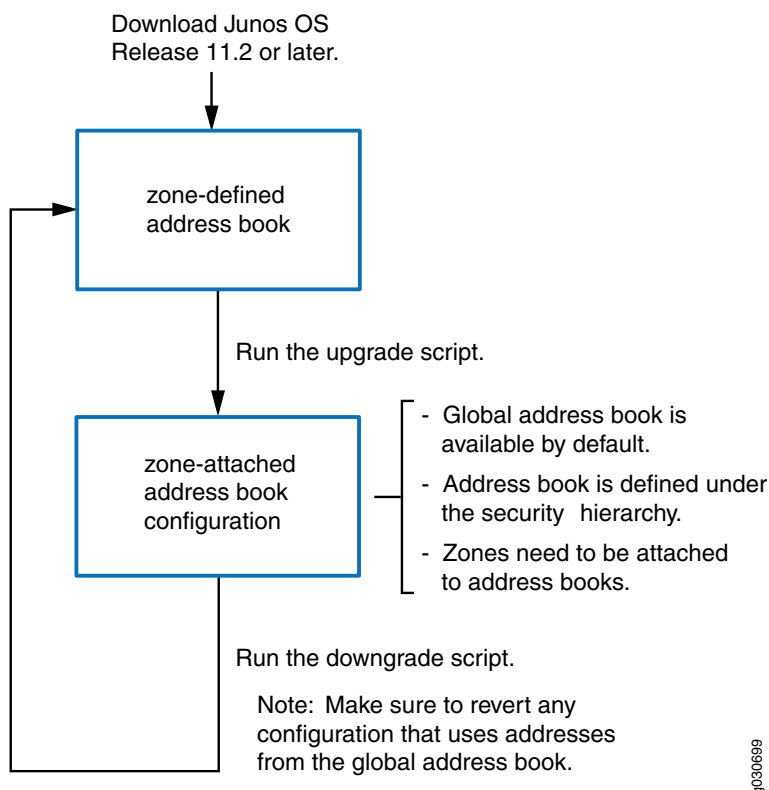
- You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.
- You cannot configure address books using the J-Web interface.

For information on how to configure zone-attached address books, see the Junos OS Release 12.1 documentation.

- **Use the downgrade script**—After upgrading to the zone-attached configuration, if you want to revert to the zone-defined configuration, use the downgrade script available on the Juniper Networks support site. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

NOTE: Before running the downgrade script, make sure to revert any configuration that uses addresses from the global address book.

Figure 1: Upgrade and Downgrade Scripts for Address Books



Running Upgrade and Downgrade Scripts

The following restrictions apply to the address book upgrade and downgrade scripts:

- The scripts cannot run unless the configuration on your system has been committed. Thus, if the zone-defined address book and zone-attached address book configurations are present on your system at the same time, the scripts will not run.
- The scripts cannot run when the global address book exists on your system.
- If you upgrade your device to Junos OS Release 12.1 and configure logical systems, the master logical system retains any previously configured zone-defined address book configuration. The master administrator can run the address book upgrade script to convert the existing zone-defined configuration to the zone-attached configuration. The upgrade script converts all zone-defined configurations in the master logical system and user logical systems.

NOTE: You cannot run the downgrade script on logical systems.

For information about implementing and executing Junos operation scripts, see the *Junos OS Configuration and Operations Automation Guide*.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life 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 Release 12.3X48 is an EEOL release. You can upgrade from Junos OS Release 12.1X46 to Release 12.3X48 or even from Junos OS Release 12.3X48 to Release 15.1X49-D10. For upgrading from Junos OS Release 12.1X47-D15 to Junos OS Release 15.1X49-D10, ISSU is supported. However, you cannot upgrade directly from a non-EEOL 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://support.juniper.net/support/eol/software/junos/>.

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

For information about ISSU, see the [Chassis Cluster User Guide for Security Devices](#).

SEE ALSO

[New and Changed Features | 314](#)

[Resolved Issues | 320](#)

[Product Compatibility | 327](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 328](#)

Hardware Compatibility

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

To determine the features supported on SRX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at: <https://pathfinder.juniper.net/feature-explorer/>

SEE ALSO

Resolved Issues 320
<i>Documentation Updates</i>
Migration, Upgrade, and Downgrade Instructions 324

Upgrading Using Unified ISSU

Unified in-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic. Unified in-service software upgrade is only supported by dual Routing Engine platforms. In addition, graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) must be enabled. For additional information about using unified in-service software upgrade, see the [High Availability User Guide for Routing Devices](#).

For information about ISSU support across platforms and Junos OS releases, see the [In-Service Software Upgrade \(ISSU\)](#) Web application.

Compliance Advisor

For regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

Finding More Information

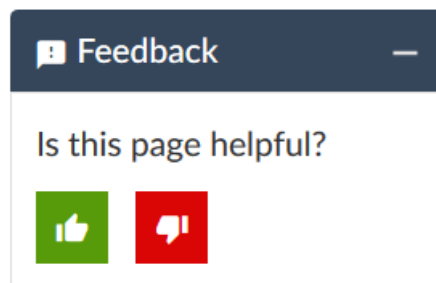
For the latest, most complete information about known and resolved issues with Junos OS, see the Juniper Networks Problem Report Search application at: <https://prsearch.juniper.net>.

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: <https://pathfinder.juniper.net/feature-explorer/>.

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

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies— For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties— For product warranty information, visit <https://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://kb.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://support.juniper.net/support/downloads/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) tool located at <https://entitlementsearch.juniper.net/entitlementsearch/welcome.do>.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <https://www.juniper.net/cm/>.
- 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, visit us at <https://support.juniper.net/support/requesting-support.html>.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net/pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to support@juniper.net. For documentation issues, fill out the bug report form located at <https://www.juniper.net/documentation/feedback/>.

Revision History

30 September 2021—Revision 24, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

26 August 2021—Revision 23, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

15 July 2021—Revision 22, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

13 January 2021—Revision 21, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

3 September 2020—Revision 20, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

8 May 2020—Revision 19, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

5 December 2019—Revision 18, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

5 September 2019—Revision 17, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

20 June 2019—Revision 16, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

19 April 2019—Revision 15, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

14 March 2019—Revision 14, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

14 February 2019—Revision 13, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

7 February 2019—Revision 12, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

11 January 2019—Revision 11, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

29 November 2018—Revision 10, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

15 November 2018—Revision 9, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

25 October 2018—Revision 8, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

4 October 2018—Revision 7, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

18 September 2018—Revision 6, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

16 August 2018—Revision 5, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

9 August 2018—Revision 4, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

6 August 2018—Revision 3, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

2 August 2018—Revision 2, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

26 July 2018—Revision 1, Junos OS Release 17.3R3— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

12 April 2018—Revision 5, Junos OS Release 17.3R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

28 February 2018—Revision 4, Junos OS Release 17.3R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

21 February 2018—Revision 3, Junos OS Release 17.3R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

15 February 2018—Revision 2, Junos OS Release 17.3R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

14 February 2018—Revision 1, Junos OS Release 17.3R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

16 November 2017—Revision 8, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

26 October 2017—Revision 7, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

23 October 2017—Revision 6, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

10 October 2017—Revision 5, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

21 September 2017—Revision 4, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

8 September 2017—Revision 3, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

1 September 2017—Revision 2, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

25 August 2017—Revision 1, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be 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.