

Release Notes: Junos[®] OS Release 18.1R2 for the ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion

26 August 2021

Contents	Introduction 11
	Junos OS Release Notes for ACX Series 11
	New and Changed Features 12
	Management 12
	Changes in Behavior and Syntax 13
	Interfaces and Chassis 13
	Known Behavior 13
	Known Issues 14
	Resolved Issues 14
	Resolved Issues: 18.1R2 15
	Resolved Issues: 18.1R1 15
	Documentation Updates 16
	New Simplified Documentation Architecture 16
	Migration, Upgrade, and Downgrade Instructions 17
	Upgrade and Downgrade Support Policy for Junos OS Releases 17

Product Compatibility | 18

Hardware Compatibility | 18

Junos OS Release Notes for EX Series Switches | 19

New and Changed Features | 19

Release 18.1R2 New and Changed Features | 20

Release 18.1R1 New and Changed Features | 22

Changes in Behavior and Syntax | 27

Interfaces and Chassis | 28

Management | 28

Multicast | 29

Network Management and Monitoring | 29

Known Behavior | 30

Infrastructure | 30

Platform and Infrastructure | 30

Known Issues | 31

General Routing | 31

Infrastructure | 33

Interfaces and Chassis | 34

Layer 2 Features | 34

Platform and Infrastructure | 34

Spanning Tree Protocols | 34

Resolved Issues | 35

Resolved Issues: 18.1R2 | 35

Resolved Issues: 18.1R1 | 37

Documentation Updates | 41

New Simplified Documentation Architecture | 41

Migration, Upgrade, and Downgrade Instructions | 42

Upgrade and Downgrade Support Policy for Junos OS Releases | 42

Product Compatibility | 43

Hardware Compatibility | 43

Junos OS Release Notes for Junos Fusion Data Center | 44

New and Changed Features | 45

Junos Fusion Data Center | 45

Changes in Behavior and Syntax | 49

Known Behavior | 49**Junos Fusion Data Center | 50****Known Issues | 50****Resolved Issues | 51****Resolved Issues: 18.1R2 | 51****Resolved Issues: 18.1R1 | 51****Documentation Updates | 52****New Simplified Documentation Architecture | 52****Migration, Upgrade, and Downgrade Instructions | 53****Basic Procedure for Upgrading an Aggregation Device | 53****Preparing the Switch for Satellite Device Conversion | 55****Configuring Satellite Device Upgrade Groups | 57****Converting a Satellite Device to a Standalone Device | 58****Upgrade and Downgrade Support Policy for Junos OS Releases | 59****Downgrading from Junos OS Release 18.1 | 59****Product Compatibility | 60****Hardware and Software Compatibility | 60****Hardware Compatibility Tool | 60****Junos OS Release Notes for Junos Fusion Enterprise | 61****New and Changed Features | 61****Junos Fusion Enterprise | 62****Changes in Behavior and Syntax | 62****Known Behavior | 63****Known Issues | 63****Junos Fusion Enterprise | 64****Resolved Issues | 64****Resolved Issues: 18.1R2 | 65****Resolved Issues: 18.1R1 | 65****Documentation Updates | 66****New Simplified Documentation Architecture | 66****Migration, Upgrade, and Downgrade Instructions | 67****Basic Procedure for Upgrading Junos OS on an Aggregation Device | 67****Upgrading an Aggregation Device with Redundant Routing Engines | 69****Preparing the Switch for Satellite Device Conversion | 70**

	Converting a Satellite Device to a Standalone Switch 71
	Upgrade and Downgrade Support Policy for Junos OS Releases 71
	Downgrading from Junos OS Release 18.1 72
Product Compatibility 72	
	Hardware and Software Compatibility 73
	Hardware Compatibility Tool 73
Junos OS Release Notes for Junos Fusion Provider Edge 74	
New and Changed Features 74	
	Release 18.1R2 New and Changed Features 75
	Release 18.1R1 New and Changed Features 75
Changes in Behavior and Syntax 76	
Known Behavior 77	
	Junos Fusion 77
Known Issues 78	
	Junos Fusion 79
Resolved Issues 80	
	Resolved Issues: 18.1R2 80
	Resolved Issues: 18.1R1 81
Documentation Updates 81	
	New Simplified Documentation Architecture 82
Migration, Upgrade, and Downgrade Instructions 82	
	Basic Procedure for Upgrading an Aggregation Device 83
	Upgrading an Aggregation Device with Redundant Routing Engines 85
	Preparing the Switch for Satellite Device Conversion 86
	Converting a Satellite Device to a Standalone Device 87
	Upgrading an Aggregation Device 87
	Upgrade and Downgrade Support Policy for Junos OS Releases 87
	Downgrading from Junos OS Release 18.1 88
Product Compatibility 89	
	Hardware Compatibility 89

Junos OS Release Notes for MX Series 3D Universal Edge Routers | 90

New and Changed Features | 90

Release 18.1R2 New and Changed Features | 91

Release 18.1R1 New and Changed Features | 91

Changes in Behavior and Syntax | 110

EVPNs | 110

High Availability (HA) and Resiliency | 111

Interfaces and Chassis | 111

Management | 112

MPLS | 112

Network Management and Monitoring | 112

Network Operations and Troubleshooting Automation | 113

Routing Protocols | 113

Software Defined Networking | 113

Subscriber Management and Services | 114

User Interface and Configuration | 115

Known Behavior | 115

EVPN | 116

General Routing | 116

Interfaces and Chassis | 117

MPLS | 118

Platform and Infrastructure | 118

Routing Protocols | 118

Services Applications | 118

Software Installation and Upgrade | 118

Known Issues | 119

EVPN | 120

Forwarding and Sampling | 121

General Routing | 121

Infrastructure | 123

Interfaces and Chassis | 124

Layer 2 Features | 124

MPLS | 125

Platform and Infrastructure | 125

- Routing Protocols | **126**
- Services Applications | **127**
- Subscriber Access Management | **127**
- VPNs | **128**

Resolved Issues | **128**

- Resolved Issues: 18.1R2 | **129**
- Resolved Issues: 18.1R1 | **136**

Documentation Updates | **154**

- New Simplified Documentation Architecture | **154**

Migration, Upgrade, and Downgrade Instructions | **155**

- Basic Procedure for Upgrading to Release 18.1 | **156**
- Procedure to Upgrade to FreeBSD 11.x based Junos OS | **156**
- Procedure to Upgrade to FreeBSD 6.x based Junos OS | **158**
- Upgrade and Downgrade Support Policy for Junos OS Releases | **160**
- Upgrading a Router with Redundant Routing Engines | **161**
- Downgrading from Release 18.1 | **161**

Product Compatibility | **162**

- Hardware Compatibility | **162**

Junos OS Release Notes for NFX Series | **163**

New and Changed Features | **163**

- Release 18.1R2 New and Changed Features | **164**
- Release 18.1R1 New and Changed Features | **164**

Changes in Behavior and Syntax | **167**

- CLI | **168**

Known Behavior | **168**

- Known Behavior: 18.1R2 | **169**

Known Issues | **170**

- Known Issues: 18.1R2 | **170**

Resolved Issues | **173**

- Resolved Issues: 18.1R2 | **173**
- Resolved Issues: 18.1R1 | **174**

Documentation Updates | **175**

- New Simplified Documentation Architecture | **175**

Migration, Upgrade, and Downgrade Instructions | 176

Upgrade and Downgrade Support Policy for Junos OS Releases | 176

Basic Procedure for Upgrading to Release 18.1 | 176

Product Compatibility | 179

Hardware Compatibility | 179

Software Version Compatibility | 180

Junos OS Release Notes for PTX Series Packet Transport Routers | 182

New and Changed Features | 182

Release 18.1R2 New and Changed Features | 183

Release 18.1R1 New and Changed Features | 183

Changes in Behavior and Syntax | 190

Interfaces and Chassis | 190

Management | 192

Network Management and Monitoring | 192

Network Operations and Troubleshooting Automation | 192

Known Behavior | 193

General Routing | 193

Interfaces and Chassis | 194

Known Issues | 194

General Routing | 195

Infrastructure | 196

Interfaces and Chassis | 196

MPLS | 196

Resolved Issues | 196

Resolved Issues: 18.1R2 | 197

Resolved Issues: 18.1R1 | 198

Documentation Updates | 201

New Simplified Documentation Architecture | 201

Migration, Upgrade, and Downgrade Instructions | 202

Upgrade and Downgrade Support Policy for Junos OS Releases | 202

Upgrading a Router with Redundant Routing Engines | 203

Basic Procedure for Upgrading to Junos OS Release 18.1 | 203

Product Compatibility | 206

Hardware Compatibility | 206

Junos OS Release Notes for the QFX Series | 207

New and Changed Features | 208

Release 18.1R2 New and Changed Features | 208

Release 18.1R1 New and Changed Features | 209

Changes in Behavior and Syntax | 227

Interfaces and Chassis | 227

Management | 227

Network Management and Monitoring | 228

Network Operations and Troubleshooting Automation | 228

Routing Policy and Firewall Filters | 229

Known Behavior | 229

EVPN | 230

Interfaces and Chassis | 230

Junos Fusion Provider Edge | 230

Layer 2 Features | 231

Multicast | 231

Platform and Infrastructure | 231

Routing Protocols | 233

Services Applications | 234

Storage and Fibre Channel | 234

Known Issues | 234

EVPN | 235

Interfaces and Chassis | 235

Layer 2 Features | 235

MPLS | 235

Platform and Infrastructure | 236

Routing Protocols | 239

Resolved Issues | 240

Resolved Issues: 18.1R2 | 240

Resolved Issues: 18.1R1 | 243

Documentation Updates | 248

New Simplified Documentation Architecture | 248

Migration, Upgrade, and Downgrade Instructions | 249

Upgrading Software on QFX Series Switches | 250

Installing the Software on QFX10002-60C Switches | 252

Installing the Software on QFX10002 Switches | 252

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 | 253

Installing the Software on QFX10008 and QFX10016 Switches | 255

Performing a Unified ISSU | 259

Preparing the Switch for Software Installation | 260

Upgrading the Software Using Unified ISSU | 260

Upgrade and Downgrade Support Policy for Junos OS Releases | 262

Product Compatibility | 263

Hardware Compatibility | 263

Junos OS Release Notes for SRX Series | 264

New and Changed Features | 265

Release 18.1R2 New and Changed Features | 265

Release 18.1R1 New and Changed Features | 265

Changes in Behavior and Syntax | 271

Chassis Cluster | 271

IDP | 271

Known Behavior | 272

Chassis Clustering | 272

Interfaces and Chassis | 272

J-Web | 273

Platform and Infrastructure | 273

Software Installation and Upgrade | 274

User Interface and Configuration | 274

VPNs | 274

Known Issues | 274

Chassis Clustering | 275

Class of Service (CoS) | 275

Flow-Based and Packet-Based Processing | 275

Intrusion Detection and Prevention (IDP) | 275

Software Installation and Upgrade | 276

	VPNs 276
Resolved Issues 276	
	Resolved Issues: 18.1R2 277
	Resolved Issues: 18.1R1 279
Documentation Updates 285	
	New Simplified Documentation Architecture 285
Migration, Upgrade, and Downgrade Instructions 286	
	Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases 286
Product Compatibility 287	
	Hardware Compatibility 287
Third-Party Components 289	
Upgrading Using ISSU 289	
Compliance Advisor 289	
Finding More Information 289	
Documentation Feedback 290	
Requesting Technical Support 291	
	Self-Help Online Tools and Resources 291
	Opening a Case with JTAC 292
Revision History 292	

Introduction

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

These release notes accompany Junos OS Release 18.1R2 for the ACX Series, EX Series, MX Series, NFX 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 | 13
- Known Behavior | 13
- Known Issues | 14
- Resolved Issues | 14
- Documentation Updates | 16
- Migration, Upgrade, and Downgrade Instructions | 17
- Product Compatibility | 18

These release notes accompany Junos OS Release 18.1R2 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/software/junos/>.

New and Changed Features

IN THIS SECTION

- [Management | 12](#)

This section describes the features and enhancements in Junos OS Release 18.1R2 for ACX Series routers.

Management

- **Support for NETCONF over SSH and custom YANG models (ACX Series)**—Starting in Junos OS Release 18.1R1, ACX Series routers support NETCONF OVER SSH and custom YANG models.

Client applications can access the NETCONF server using the SSH protocol and use the standard SSH authentication mechanism. After authentication, the NETCONF server uses the configured Junos OS login usernames and classes to determine whether a client application is authorized to make each request.

You can load custom YANG models on the router 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. You can load custom YANG modules by using the **request system yang add** operational command.

[See [Understanding the Management of Nonnative YANG Modules on Devices Running Junos OS.](#)]

SEE ALSO

- [Changes in Behavior and Syntax | 13](#)
- [Known Behavior | 13](#)
- [Documentation Updates | 16](#)
- [Known Issues | 14](#)
- [Resolved Issues | 14](#)
- [Migration, Upgrade, and Downgrade Instructions | 17](#)
- [Product Compatibility | 18](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [Interfaces and Chassis | 13](#)

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 18.1R2 for the ACX Series routers.

Interfaces and Chassis

- **Modified output of show-ptp-clock command (QFX Series switches)**—Starting in Junos OS Release 18.1R1, the output of the **show-ptp-clock** command is modified to display the value of the **GMC Class** field as **248** for a PTP boundary clock when the lock state of the clock is **Acquiring**.

SEE ALSO

[New and Changed Features | 12](#)[Known Behavior | 13](#)[Documentation Updates | 16](#)[Known Issues | 14](#)[Resolved Issues | 14](#)[Migration, Upgrade, and Downgrade Instructions | 17](#)[Product Compatibility | 18](#)

Known Behavior

There are no known limitations in Junos OS Release 18.1R2 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 13
Documentation Updates 16
Known Issues 14
Resolved Issues 14
Migration, Upgrade, and Downgrade Instructions 17
Product Compatibility 18

Known Issues

There are no known issues in hardware and software in Junos OS Release 18.1R2 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 13
Known Behavior 13
Documentation Updates 16
Resolved Issues 14
Migration, Upgrade, and Downgrade Instructions 17
Product Compatibility 18

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 18.1R2 | 15](#)
- [Resolved Issues: 18.1R1 | 15](#)

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: 18.1R2

There are no resolved issues in Junos OS 18.1R2 Release for ACX Series routers.

Resolved Issues: 18.1R1

Alarms

- The major alarm about Fan & PSU Airflow direction mismatch was seen by removing management cable [PR1327561](#)

Dynamic Host Configuration Protocol

- ACX5000 line of routers did not forward DHCP-RELAY requests with IRB interface after upgrade. [PR1243687](#)

Firewall Filters

- On ACX Series routers, syslog error was seen on the output/egress firewall filter. [PR1316588](#)

Installation and Upgrade

- fxpc core was observed during ISSU upgrade. [PR1318771](#)

Layer 2 Features

- On ACX5000 line of routers, transit ARP packets were being punted to the RE. [PR1263012](#)

VPN

- On ACX5000 line of routers, memory leak was seen during Layer 3 VPN scaling test when committing Layer 3 VPN configuration. [PR1115686](#)

SEE ALSO

New and Changed Features 12
Changes in Behavior and Syntax 13
Known Behavior 13
Documentation Updates 16
Known Issues 14
Migration, Upgrade, and Downgrade Instructions 17

Documentation Updates

IN THIS SECTION

- [New Simplified Documentation Architecture | 16](#)

There are no errata or changes in Junos OS Release 18.1R2 for the ACX Series documentation.

New Simplified Documentation Architecture

- With the release of Junos OS Release 18.1, Juniper is simplifying its technical documentation to make it easier for you to find information and know that you can rely on it when you find it. In the past, we organized documentation about Junos OS software features into platform-specific documents. In many cases, features are supported on multiple platforms, so you might not easily find the document you want for your platform.

With Junos OS Release 18.1, we have eliminated the platform-specific software feature documents. For example, if you want to find documentation on OSPF, there is only one document regardless of which platform you have. Here are some of the benefits of our new simplified architecture:

- Over time, you will see better search results when looking for Juniper documentation. You will be able to find what you want faster and be assured that is the right document.
- If a software feature is supported on multiple platforms, you can find information about all the platforms in one place.
- Because we have eliminated many documents that covered similar topics, you will now find one document with all the information.
- You can know that you are always getting the most current and accurate information.

SEE ALSO

[New and Changed Features | 12](#)

[Changes in Behavior and Syntax | 13](#)

[Known Behavior | 13](#)

[Known Issues | 14](#)

[Resolved Issues | 14](#)

[Migration, Upgrade, and Downgrade Instructions | 17](#)

[Product Compatibility | 18](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 17](#)

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

For information about software installation and upgrade, see the [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 17.1, 17.2 and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

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 13
Known Behavior 13
Documentation Updates 16
Known Issues 14
Resolved Issues 14
Product Compatibility 18

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 18

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 13
Known Behavior 13

Documentation Updates | 16

Known Issues | 14

Resolved Issues | 14

Migration, Upgrade, and Downgrade Instructions | 17

Junos OS Release Notes for EX Series Switches

IN THIS SECTION

- New and Changed Features | 19
- Changes in Behavior and Syntax | 27
- Known Behavior | 30
- Known Issues | 31
- Resolved Issues | 35
- Documentation Updates | 41
- Migration, Upgrade, and Downgrade Instructions | 42
- Product Compatibility | 43

These release notes accompany Junos OS Release 18.1R2 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/software/junos/>.

New and Changed Features

IN THIS SECTION

- Release 18.1R2 New and Changed Features | 20
- Release 18.1R1 New and Changed Features | 22

This section describes the new features and enhancements to existing features in Junos OS Release 18.1R2 for the EX Series.

NOTE: The following EX Series switches are supported in Release 18.1R2: EX2300, EX3400, EX4300, EX4600, and EX9200.

NOTE: In Junos OS Release 18.1R2, J-Web is supported on the EX2300, EX3400, 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 [J-Web Application Package Release 18.1A1 for EX2300, EX3400, EX4300 and EX4600 Switches](#).

Release 18.1R2 New and Changed Features

Hardware

- **EX2300-24MP and EX2300-48MP switches**—Starting with Junos OS Release 18.1R2, two new models of EX2300 switches—EX2300-24MP and EX2300-48MP—are available. EX2300-24MP switch models have eight 100/1000/2500 BASE-T Gigabit Ethernet ports with PoE/PoE+ capability, 16 10/100/1000 BASE-T Gigabit Ethernet ports with PoE/PoE+ capability, and four built-in 10-Gigabit Ethernet uplink ports. EX2300-48MP switch models have 16 100/1000/2500 BASE-T Gigabit Ethernet ports with PoE/PoE+ capability, 32 10/100/1000 BASE-T Gigabit Ethernet ports with PoE/PoE+ capability, and six built-in 10-Gigabit Ethernet uplink ports.

[See [EX2300 Switch Hardware Guide](#).]

Interfaces and Chassis

- **Support for Multi-Gigabit Ethernet (EX2300)**—Starting in Junos OS Release 18.1R2, the Multi-Gigabit Ethernet feature is supported on EX2300-48MP and EX2300-24MP switches. This feature fulfills the high-speed requirements for a large and mid-size campus, and branch locations for the enterprise customers.

The **mge** interface is a rate-selectable (multirate) Gigabit Ethernet interface that can support speeds of 10 Gbps, 5 Gbps, and 2.5 Gbps over CAT5e/CAT6/CAT6a cables. In the EX2300, the **mge** interface

supports 100 Mbps, 1 Gbps, and 2.5 Gbps speeds, which can be configured by using the **speed** configuration statement.

NOTE: Power over Ethernet (PoE) is supported on Multi-Gigabit Ethernet interfaces. PoE enables EX2300 switches to transfer electrical power through an Ethernet cable. PoE enables electric power, along with data, to be passed over a copper Ethernet LAN cable.

[See [Speed](#).]

- **Support for Power over Ethernet (EX2300-24MP and EX2300-48MP)**—Starting in Junos OS Release 18.1R2, Power over Ethernet (PoE) is supported on EX2300-24MP and EX2300-48MP switch models, including multigigabit interfaces. (PoE) permits electric power, along with data, to be passed over a copper Ethernet LAN cable.

EX2300 24MP switches support PoE (IEEE 802.3af) and PoE+ (IEEE 802.3at) and can simultaneously deliver up to 15.4 watts of standards-based 802.3af Class 3 PoE to a maximum of 24 ports or 30 watts of standards-based 802.3at PoE+ to a maximum of 12 ports, based on a total system budget of 380 watts.

EX2300 48MP switches support PoE (IEEE 802.3af) and PoE+ (IEEE 802.3at) and can simultaneously deliver up to 15.4 watts of standards-based 802.3af Class 3 PoE to a maximum of 48 ports or 30 watts of standards-based 802.3at PoE+ to a maximum of 24 ports, based on a total system budget of 740 watts.

[See [Understanding PoE on EX Series Switches](#).]

Virtual Chassis

- **Virtual Chassis support (EX2300-24MP and EX2300-48MP)**—Starting in Junos OS Release 18.1R2, multigigabit EX2300 switches can be interconnected into a Virtual Chassis and operate as one logical device managed as a single chassis, as follows:
 - Members can be any combination of up to four EX2300-24MP and EX2300-48MP switches.
 - Multigigabit EX2300 switches cannot be mixed with any other switch models (including any other EX2300 switches) in the same Virtual Chassis.
 - Any 10-Gbps uplink ports installed with SFP+ transceivers can be configured as Virtual Chassis ports (VCPs) to interconnect the members. Multigigabit EX2300 switches do not have any dedicated or default-configured VCPs.

To configure a multigigabit EX2300 Virtual Chassis, use similar steps as for configuring other EX Series and QFX Series Virtual Chassis.

[See [Understanding EX2300 Virtual Chassis.](#)]

Release 18.1R1 New and Changed Features

Hardware

- **EX9251 switches**—Starting with Junos OS Release 18.1R1, EX9251 switches are available as a fixed configuration switch. It is an Ethernet-optimized switch that provides carrier-class Ethernet switching. It has a throughput of up to 400 gigabits per second (Gbps). The switch is available in two variants—with AC power supply and with DC power supply.

[See [EX9251 Switch Hardware Guide.](#)]

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

- **Access control and authentication (EX2300 and EX3400 switches)**—Starting with Junos OS Release 18.1R1, EX2300 and EX3400 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 authenticate 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.

This feature was introduced previously in an “X” release of Junos OS.

[See [Understanding Authentication on Switches.](#)]

- **TACACS+ authorization for operational commands using regular expressions (EX2300, EX3400, EX4300 switches and MX Series)**—Starting in Junos OS Release 18.1R1, you can configure authorizations for operational mode commands using regular expressions using the **allow-commands-regexps** and **deny-commands-regexps** statements. Authorizations can also be configured remotely by specifying Juniper Networks vendor-specific attributes (VSAs) in your TACACS+ authentication server's configuration.

[See [Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies.](#)]

Class of Service (CoS)

- **Support for Class of service (EX2300 and EX3400 switches and EX3400 Virtual Chassis)**—Starting in Junos OS Release 18.1R1, when a packet traverses a switch, the switch provides the appropriate level of service to the packet using either default class-of-service(CoS) settings or CoS settings that you configure. On ingress ports, the switch classifies packets into appropriate forwarding classes and assigns a loss priority to the packets. On egress ports, the switch applies packet scheduling and any rewrite rules to re-mark packets.

This feature was previously supported in an “X” release of Junos OS.

[See [Junos OS CoS for EX Series Switches Overview](#).]

High Availability (HA) and Resiliency

- **High availability features (EX3400 switches and EX3400 Virtual Chassis)**—Starting with Junos OS Release 18.1R1, high availability features are supported. High availability features refer to the hardware and software components that provide redundancy and reliability for network communications.

The following features are supported:

- Graceful Routing Engine switchover (GRES), nonstop active routing and nonstop bridging
- Virtual Router Redundancy Protocol (VRRP) support

VRRP enables you to provide alternative gateways for end hosts that are configured with static default routes. You can implement VRRP to provide a high availability default path to a gateway without the need to configure dynamic routing or router discovery protocols on end hosts.

[See [High Availability User Guide](#).]

Layer 2 Features

- **Layer 2 features (EX3400 switches and EX3400 Virtual Chassis)**—Starting with Junos OS Release 18.1R1, the following Layer 2 features are supported:

- VLAN support

VLANs enable you to divide one physical broadcast domain into multiple virtual domains.

- Link Layer Discovery Protocol (LLDP) support

LLDP enables a switch to advertise its identity and capabilities on a LAN, as well as receive information about other network devices.

- Q-in-Q tunneling support

This feature enables service providers on Ethernet access networks to extend a Layer 2 Ethernet connection between two customer sites.

- Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP) support

These protocols enable a switch to advertise its identity and capabilities on a LAN and receive information about other network devices.

This feature was previously supported in an “X” release of Junos OS.

[See [Ethernet Switching User Guide](#).]

Layer 3 Features

- **Layer 3 feature support (EX2300 and EX3400 Switches)**—Starting with Junos OS Release 18.1R1, the Layer 3 features supported in Junos OS Release 15.1X53-D50 are now supported on EX2300 and EX4300 Switches.

Multicast

- **Layer 2 and Layer 3 multicast support (EX2300 switches and Virtual Chassis, EX3400 switches and Virtual Chassis)**—Starting in Junos OS Release 18.1R1, the following IPv4 and IPv6 multicast protocols are supported:
 - Internet Group Management Protocol (IGMP) v1, v2, and v3
 - IGMP snooping
 - Multicast Listener Discovery (MLD) protocol v1 and v2
 - MLD snooping
 - Multicast Source Discovery Protocol (MSDP)
 - Protocol Independent Multicast (PIM) sparse mode (SM), dense mode (DM), and source-specific multicast (SSM)

These features were previously supported in an “X” release of Junos OS.

[See [Multicast Protocols User Guide](#).]

Network Management and Monitoring

- **Pseudohardware RPM timestamps (EX4300 switches and EX4300 Virtual Chassis)**—Starting in Junos OS Release 18.1R1, you can configure a pseudo-hardware timestamp on the switch for real-time performance monitoring (RPM). RPM enables you to configure active probes to track and monitor traffic on the network. To achieve this, RPM exchanges a set of probes with other IP hosts in the network. These probes are sent from a source node to other destination devices in the network that requires tracking. To account for latency or jitter in the communication of probe messages, you can enable timestamping of the probe packets. On the EX4300 switch, RPM timestamping is performed in the software. The RPM probes at the requester and responder devices are timestamped in the Packet Forwarding Engine instead of the Junos OS process (rmpod) that runs on the Routing Engine. This timestamping method is referred to as pseudo-hardware timestamping. You must configure the switch as both the RPM client (the requester) and the RPM server (the responder) to timestamp the RPM packet. You configure pseudohardware timestamps at the `[edit services rpm]` hierarchy level.

[See [Understanding Real-Time Performance Monitoring on EX Series Switches](#).]

- **Port mirroring support (EX2300, EX2300-C, and EX3400 switches and EX3400 Virtual Chassis)**—Starting in Junos OS Release 18.1R1, port mirroring is supported on EX2300, EX2300-C, and EX3400 switches and EX3400 Virtual Chassis. 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, and correlating events.

This feature was previously supported in an “X” release of Junos OS.

[See [Understanding Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches.](#)]

Port Security

- **IPv4/IPv6 source guard (EX4600 switches)**—Starting in Junos OS Release 18.1R1, 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. This feature is supported for IPv4 and IPv6 source addresses.

[See [Understanding IP Source Guard for Port Security on EX Series Switches.](#)]

- **MACsec license enforcement (EX3400, EX4300, EX4600, EX9200, QFX5100 switches and Junos Fusion Enterprise)**—Starting in Junos OS Release 18.1R1, Media Access Control Security (MACsec) requires the installation of a MACsec feature license. If the MACsec license is not installed, MACsec functionality cannot be activated. You add the MACsec license using the **request system license add** command.

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

Security

- **Distributed denial-of-service (DDoS) protection (EX2300 and EX3400 switches, EX2300 and EX3400 Virtual Chassis)**—Starting in Junos OS Release 18.1R1, you can configure DDoS protection that enables the switch to continue functioning while under attack. DDoS attacks use multiple sources to flood a network or switch with protocol control packets. This malicious traffic triggers a large number of exceptions in the network and tries to exhaust the system resources so that valid users are denied access to the network or server. DDoS protection identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed.

[See [Distributed Denial-of-Service \(DDoS\) Protection Overview.](#)]

- **Support for firewall filters (EX2300 and EX3400 switches, EX2300 and EX3400 Virtual Chassis)**—Starting in Junos OS Release 18.1R1, you can define firewall filters on the switch 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.

This feature was previously supported in an “X” release of Junos OS.

[See [Firewall Filters for EX Series Switches Overview.](#)]

- **Port security features (EX2300 and EX3400 switches, EX2300 and EX4300 Virtual Chassis)**—Starting in Junos OS Release 18.1R1, the following port security features are supported:

- DHCP snooping (Pv4 and IPv6)—Filters and blocks ingress Dynamic Host Configuration Protocol (DHCP) server messages on untrusted ports, and builds and maintains a database of DHCP lease information, which is called the DHCP snooping database.
- Dynamic ARP inspection (DAI)—Prevents Address Resolution Protocol (ARP) spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable DAI on a VLAN.
- IPv6 neighbor discovery inspection—Prevents IPv6 address spoofing attacks. Neighbor discovery requests and replies are compared against entries in the DHCPv6 snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable neighbor discovery inspection on a VLAN.

This feature was previously supported in an “X” release of Junos OS.

[See [Understanding Port Security Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity](#).]

- **Port mirroring to IP address (EX4600 switches and Virtual Chassis)**—Starting with Junos OS Release 18.1R1, you can send mirrored packets to an IP address over a Layer 3 network (for example, if there is no Layer 2 connectivity to the analyzer device).

[See [Understanding Port Mirroring](#).]

User Interface and Configuration

- **Support for configuring the ephemeral database using the NETCONF and Junos XML protocols (EX2300, EX3400, EX4300, EX4600, and EX9200 switches)**—Starting in Junos OS Release 18.1R1, NETCONF and Junos XML protocol client applications can configure the ephemeral configuration database. The ephemeral database provides a fast programmatic interface 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](#).]

Virtual Chassis

- **Virtual Chassis support (EX2300, EX3400)**—Starting in Junos OS Release 18.1R1, EX2300 or EX3400 switches can be interconnected into a Virtual Chassis and operate as one logical device managed as a single chassis, as follows:
 - EX2300 Virtual Chassis: Up to four EX2300 and EX2300-C member switches, interconnected using any 10-Gbps SFP+ ports configured as Virtual Chassis ports (VCPs)
 - EX3400 Virtual Chassis: Up to 10 EX3400 member switches, interconnected using the QSFP+ uplink ports (default-configured VCPs) or any SFP+ uplink ports configured as VCPs

To configure an EX2300 or EX3400 Virtual Chassis, use similar steps as for configuring other EX Series and QFX Series Virtual Chassis.

This feature was previously supported in an “X” release of Junos OS.

[See [Virtual Chassis User Guide for Switches](#).]

SEE ALSO

Changes in Behavior and Syntax	 27
Known Behavior	 30
Known Issues	 31
Resolved Issues	 35
Documentation Updates	 41
Migration, Upgrade, and Downgrade Instructions	 42
Product Compatibility	 43

Changes in Behavior and Syntax

IN THIS SECTION

- [Interfaces and Chassis](#) | 28
- [Management](#) | 28
- [Multicast](#) | 29
- [Network Management and Monitoring](#) | 29

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 18.1R2 for the EX Series.

Interfaces and Chassis

- **EEE not supported on mge interfaces operating at 100-Mbps speed (EX2300-24MP and EX2300-48MP)**—In Junos OS Releases 18.1R2, if both Energy Efficient Ethernet (EEE) and 100-Mbps speed are configured on a rate-selectable (or multirate) Gigabit Ethernet (mge) port on EX2300-24MP and EX2300-48MP switches, the port operates only at 100-Mbps speed but EEE is not enabled on that port. EEE is supported only on mge interfaces that operate at 1-Gbps and 2.5-Gbps speeds.

Management

- **Enhancement to NPU memory sensors for Junos Telemetry Interface (EX9200 switches)**—Starting with Junos OS Release 18.1R1, the format of telemetry data exported through gRPC for NPU memory and memory utilization implements prefix compression. This change reduces the payload size of data exported. The following example shows the new format:

key: __prefix__

str_value: /components/component[name='FPC0:NPU0']/properties/property

key: [name='mem-util-edmem-size']/value

uint_value: 12345

Telemetry data is exported in key-value pairs. Previously, the data exported included the component and property names in a single key string.

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

- **Enhancement to LSP statistics sensor for Junos Telemetry Interface (EX9200 switches, QFX10000 switches, MX Series, and PTX Series)**—Starting with Junos OS 18.1R1, the telemetry data exported for the LSP statistics sensor no longer includes the phrase **and source 0.0.0.0** after the LSP name in the value string for the prefix key. This change reduces the payload size of data exported. The following is an example of the new format:

str_value: /mpls/lsp/constrained-path/tunnels/tunnel[name='LSP-4-3']/state/
counters[name='c-27810']/

Multicast

- **Support for per-source multicast traffic forwarding with IGMPv3 (EX4300)**—Starting in Junos OS Release 18.1R2, EX4300 switches forward multicast traffic on a per-source basis according to received IGMPv3 INCLUDE and EXCLUDE reports. In releases prior to these releases, 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

- **SNMP syslog messages changed (EX Series)**—Starting in Junos OS Release 18.1R1, 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](#).]

SEE ALSO

New and Changed Features	19
Known Behavior	30
Known Issues	31
Resolved Issues	35
Documentation Updates	41
Migration, Upgrade, and Downgrade Instructions	42
Product Compatibility	43

Known Behavior

IN THIS SECTION

- [Infrastructure | 30](#)
- [Platform and Infrastructure | 30](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.1R2 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.

Infrastructure

- When the image is copied through FTP from a server to a switch, sometimes the ftpd WCPU might go high, causing the CLI to freeze for approximately 10 seconds. [PR1306286](#)
- On rare occasions, the EX2300-MP switch panics with fatal abort. This issue is seen when the rpd process is aborted and it occurs only when dtrace is enabled with continuous rpd process killing. [PR1329552](#)

Platform and Infrastructure

- On EX4300 switches, when 802.1X single-supplicant authentication is initiated, multiple **EAP Request Id Frame Sent** packets might be sent. [PR1163966](#)
- On EX4300 10G links, preexisting MACsec sessions might not come up after the following events (1) Process (pfex, dot1x) restarts or the system restarts. (2) The link flaps. [PR1294526](#)
- LAG interfaces flap during unified ISSU when fast LACP timers are configured. This might result in traffic loss during the unified ISSU. This issue occurs because Fast LACP timers are not supported on EX-92XX during unified ISSU. The fast LACP timer support needs to be added. [PR1316251](#)
- NSSU upgrade from Junos OS Release 15.1X53-D58 to Junos OS Release 18.1R1 will fail with ksyncd core in backup Routing Engine. [PR1344686](#)
- When upgrading from certain release to Junos OS Release 18.1R1 statistics daemon PFED might be seen generating core files. This issue is not service impacting. The issue can be cleared by rebooting the chassis or by deleting all files from /mfs. [PR1346925](#)

SEE ALSO

New and Changed Features	19
Changes in Behavior and Syntax	27
Known Issues	31
Resolved Issues	35
Documentation Updates	41
Migration, Upgrade, and Downgrade Instructions	42
Product Compatibility	43

Known Issues

IN THIS SECTION

- General Routing | 31
- Infrastructure | 33
- Interfaces and Chassis | 34
- Layer 2 Features | 34
- Platform and Infrastructure | 34
- Spanning Tree Protocols | 34

This section lists the known issues in hardware and software in Junos OS Release 18.1R2 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

- 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 EX Series Virtual Chassis platforms, the interface MAC address might not be restored after deleting or rolling back the configuration. As a result, the hardware address and current address might not be the same. [PR1319234](#)

- On an EX3400 platform, when **force-renew** is initiated from a server, the renewing entry for the bounded client will not be displayed under **show dhcp-security binding**. [PR1328542](#)
- On an EX2300-48P, the port ge-0/0/16-23 does not advertise a 10-Mbps speed. It advertises only 100 and 1000-Mbps speeds. [PR1331357](#)
- When a restart chassis-control is done for the first time after the software image is upgraded or after the switch is rebooted, the MPC booting state changes from offline to online directly, without staying at present state during booting. This issue is not seen consistently. There is no functional impact because of this state change. [PR1332613](#)
- On an EX9251 switch, physical links might not come up if you perform frequent port profile changes while a line card reboot is in progress. [PR1340140](#)
- On EX2300 and EX3400 platforms, when the bulk of MAC notifications are received along with **interface-mac-limit** configuration changes, the device might stop learning the MAC address, and the MAC address might be displayed with the **Hit Pending** status. [PR1341518](#)
- If there is a packet loop between autodiscoveries because of a redundant link, clearing DHCP relay bindings might reboot one autodiscovery in a dual autodiscovery setup. If you remove the redundant link then the reboot will not be seen. [PR1347507](#)
- On EX2300-24MP and EX2300-48MP switches, wrong number of Fan count is shown in for jnxContainersCount. Shows 4 instead of 3. There is no functionality impact. [PR1361025](#)
- On rare occasions, on EX2300-24MP and EX2300-48MP switches, in setup with scaled dot1X and DHCP client, after Master switchover, reboot, or power cycle, FXPC core is observed. After the switchover is complete and dot1x session and DHCP is rebinded, the switch recovers and sessions come up without any issues. [PR1361042](#)
- On rare occasions, on EX2300-24MP and EX2300-48MP switches, during commit of a Scaled Multi Feature configuration, there can be a CPU hog for certain thread which might lead to this watchdog to generate core files. [PR1361662](#)
- **fpc0 optic_set_activity_led:[FPC:0 PIC:0 Port:33 Chan:0 - Ifd Speed:0] Failed setting activity led to ON** these are observed on both vty and /var/log/messages when traces are enabled. These messages are seen on ports where no optics are connected and do not have any functionality impact. [PR1361739](#)
- On EX300-24MP and EX2300-48MP switches, **dc-pfe: Error:tvtp_optics_sfpt_read: Failed to read eeprom for link 1/0 & fpc0 Error:tvtp_optics_sfpt_read: Failed to read eeprom for link 1/0** transient error messages are seen in /var/log/messages for SFP-T transceivers initialisation. These are seen after the device is rebooted & they do not have any functionality impact. [PR1361751](#)
- On rare occasions, on EX2300-24MP and EX2300-48MP switches, after multiple GRES, it is observed that the PSU and Fan details for the switch in line card role is not displayed. There is no functionality impact. Reboot of line card resolves the issue. [PR1362140](#)
- During system upgrade on EX2300-24MP and EX2300-48MP switches, an instance of a switch which is stressed with multiple disc writes, power cycles, process kills etc goes to loader prompt is observed. Power cycle resolves the issue. [PR1362197](#)

- On EX2300-24MP and EX2300-48MP switches, an instance of FXPC generating core files during upgrade is observed on one setup. Complete core is not generated, the system recovers after the FXPC generates core files. [PR1362232](#)
- On a rare occasion, on EX2300-48MP switches, the **show virtual-chassis** command might not display the model name. [PR1362421](#)

Infrastructure

- Previously support for archiving a dmesg file meant only the last reboot logs were recorded. With a fix, the last three reboots are archived.

```
% ls -lh /var/run/dmesg.boot* -rw-r--r-- 1 root wheel 3.7K Dec 13 08:33 /var/run/dmesg.boot -rw-r--r-- 1 root wheel 1.8K Dec 13 08:33 /var/run/dmesg.boot.0.gz -rw-r--r-- 1 root wheel 1.8K Dec 13 08:23 /var/run/dmesg.boot.1.gz -rw-r--r-- 1 root wheel 7.1K Dec 13 08:34 /var/run/dmesg.boot.detail -rw-r--r-- 1 root wheel 3.1K Dec 13 08:34 /var/run/dmesg.boot.detail.0.gz -rw-r--r-- 1 root wheel 3.0K Dec 13 08:24 /var/run/dmesg.boot.detail.1.gz.
```

[PR1327021](#)
- In a VLAN swap case, the ARP packet processed at the switch fabric interface contains the original dsa-tag (cvid) which is derived as an invalid hw-token. For this special case, the packet is sent to the kernel. The VLAN classification or regeneration for invalid hw-token returns zero as hw-token. [PR1342432](#)
- If an EX2300-24MP or an EX2300-48MP box is unable to boot Junos and a recovery is needed, then such a recovery could be attempted in multiple ways. One of the ways is to install a usable image via USB storage medium. When USB storage medium is used to install a Junos image for recovering such a box, the installation of the image would be unsuccessful. The standard bootable medium would not have a usable Junos image. [PR1363240](#)
- On EX2300, EX2300-C, and EX2300-MP platforms, if Junos OS is with FreeBSD kernel version 11 with the build date on or after 2019-02-12, the switch might stop forwarding traffic or responding to console. A reboot is required to restore the service. [PR1442376](#)

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 was assigned with the identical address after commit. There was 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](#)

Layer 2 Features

- On rare occasions, on EX2300-24MP and EX2300-48MP switches, vmcore.live is seen during backup Routing Engine disconnection due to split-merge, renumbering, or mastership switchover. The switch will not be GRES ready post this core as back up Routing Engine would not be in sync. In order to sync, reboot the back up Routing Engine. [PR1361047](#)

Platform and Infrastructure

- On EX4300 switches, Media Access Control Security (MACsec) might not work properly on PHY84756 1G SFP ports if **auto negotiation** is on and MACsec is configured on those ports. On the EX4300 copper box, all four uplink ports (PIC 2) are attached to PHY84756. On the the EX4300 fiber box, the last four ports of the base board (PIC 0) and 8*1G/10G uplink ports (PIC 2) are attached to PHY84756. [PR1291724](#)
- On EX4300 switches, the filter-based forwarding (FBF) might not work properly after deactivating or activating. This issue occurs because stale entries are not being freed in ternary content addressable memory (TCAM), which leads to insufficient space in TCAM for processing filters. [PR1293581](#)
- On an MPC5 line card, the inline-ka PPP echo requests are not transmitted when the anchor-point is lt-x/2/x or lt-x/3/x in a pseudowire deployment. [PR1345727](#)

Spanning Tree Protocols

- On EX Series switches (except for EX4300, EX4600, and EX9200), the VoIP interfaces might be blocked by Rapid Spanning Tree Protocol (RSTP) if voice VLAN is running VLAN Spanning Tree Protocol (VSTP) and data VLAN is running RSTP, respectively. [PR1306699](#)

SEE ALSO

[New and Changed Features | 19](#)

[Changes in Behavior and Syntax | 27](#)

[Known Behavior | 30](#)

[Resolved Issues | 35](#)

[Documentation Updates | 41](#)

[Migration, Upgrade, and Downgrade Instructions | 42](#)

[Product Compatibility | 43](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 18.1R2 | 35](#)
- [Resolved Issues: 18.1R1 | 37](#)

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: 18.1R2

General Routing

- The **hawkeye alarmd** transient error is observed on MX240, MX480, MX960, EX9200, and SRX5000 platforms. [PR1312336](#)
- On an EX3400 switch, MACsec is not supported on 10G uplink ports. [PR1325545](#)
- Traffic going through the aggregated Ethernet interface might be dropped if mastership changes. [PR1327578](#)
- The EX3400 switch floods unicast ARP replies in the VLAN when dynamic ARP inspection is enabled. [PR1331928](#)
- On an EX9200 switch, when an anchor FPC has no active child, bridge protocol data units (BPDUs) are not sent out to the other active child. [PR1333872](#)
- All the DHCP-Reply or DHCP-Offer packets might be discarded by the DHCP snooping if the DHCP snooping is not enabled in that VLAN. [PR1345426](#)

- On an EX2300 running Junos OS Release 15.1X53-D56 with the fxpc process, issuing the **accept-source-mac** command causes the CPU usage to spike up to 90 percent on an idle chassis. [PR1345978](#)
- The statistics PFED process might generate a core file on an upgrade between certain releases. [PR1346925](#)
- Starting in Junos OS Release 18.1R2, there is support for OPSFv3 authentication on EX Series switches. [PR1347630](#)
- Different behavior on the tagging of interfaces before and after reboot without any change in configuration. [PR1349712](#)
- On EX2300 and EX3400 switches, the **lACP mac re-write** protocol sends duplicate Link Aggregation Control Protocol (LACP), bridge protocol data unit (BPDU) with different destination MAC addresses. [PR1350329](#)
- After an EX2300 switch reboots, if you have ECMP next hop configured, the ECMP group might only be created on one Packet Forwarding Engine. [PR1351418](#)

Forwarding and Sampling

- After an EX9251 switch is set to factory default by zeroize, the DHCP service crashes. [PR1329682](#)

Infrastructure

- EX4300 firewall rule ip-options with knobs other than "any" doesn't provide expected results. [PR1173347](#)
- On an EX4600 switch, priority-based flow control (PFC) frames might not work. [PR1322439](#)
- The **interface LED** status might stay green even after disabling the interface and removing the cable. [PR1329903](#)

Interfaces and Chassis

- Some PoE devices may not receive PoE power from EX2300 or EX3400 switches due to a false report of Underload Latch. [PR1345234](#)
- On EX4600, the MC-lag after reboot of VRRP Master and Back up discards traffic to downstream switches. [PR1345316](#)

Platform and Infrastructure

- On the EX4300 Virtual Chassis switch, the FPC might crash and a PFEX core file might get generated. [PR1261852](#)
- Multicast receiver connected to the EX4300 switch might not be able to get the multicast streaming. [PR1308269](#)
- Autonegotiation is not working as expected between EX4300 and SRX5800. [PR1311458](#)
- IGMPv3 on EX4300 does not have the correct outgoing interfaces in the Packet Forwarding Engine that are listed in the kernel. [PR1317141](#)

- On an EX4300 platform, a MAC learning issue and new VLANs creation failure might occur for some VLANs. [PR1325816](#)
- On an EX4300 platform, when exhausting TCAM, the table filter is still programmed. [PR1330148](#)
- Internet Group Management Protocol (IGMP) packets are forwarded out of the redundant trunk group (RTG) backup interface. [PR1335733](#)
- MSTP might not work normally after permitting a commit. [PR1342900](#)
- On EX4300, the loopback filter is not blocking unauthorized BGP peers. [PR1343402](#)
- The firewall filter might not be programmed in the Packet Forwarding Engine even though TCAM entries are available. [PR1345296](#)
- The VLAN translation feature does not work for the control plane traffic. [PR1348094](#)
- Traffic drop might occur if LLC packets are sent with DSAP and SSAP as 0x88 and 0x8e. [PR1348618](#)

Routing Protocols

- Open Shortest Path First (OSFP) routes cannot be added to the routing table until the **lsa-refresh** timer expires. [PR1316348](#)
- The **igmp-snooping** protocol might be enabled unexpectedly. [PR1327048](#)

Resolved Issues: 18.1R1

Authentication and Access Control

- The LLDP-MED cannot forward the correct POE class. [PR1296547](#)
- The dot1x process might stop authenticating if continuous dot1x client reauthentication requests cannot get processed. [PR1300050](#)
- EX2300-C is missing the dot1xd_usr_authenticated help string. [PR1311465](#)

EVPN

- Split horizon label is not allocated after switching the configuration of ESI from 'single-active' to 'all-active'. [PR1307056](#)

Infrastructure

- Reboot logs are not shown on the mini-USB console even though **set system ports auxiliary port-type mini-usb** is configured. [PR1192388](#)
- The file system might be corrupted multiple times during image upgrade or commit operation. [PR1317250](#)
- PFC feature might not work on EX4600. [PR1322439](#)
- The ifinfo might generate core files on the EX4600 Virtual Chassis. [PR1324326](#)

Interfaces and Chassis

- On EX2300 and EX3400 IPV6 neighborship is not created on the IRB interface. [PR1198482](#)
- On the EX4300 Virtual Chassis: LACP flap is observed, after rebooting the master FPC with PDT configurations. [PR1301338](#)
- The interface might not work properly after the FPC restarts. [PR1329896](#)

MPLS

- QFX5100 and EX4600: Unified ISSU is not supported with MPLS configuration. [PR1264786](#)

Platform and Infrastructure

- After access is rejected, the dot1x process might crash due to memory leak. [PR1160059](#)
- On EX3400 and EX2300, LLDP, LACP, and MVRP protocols are not available under the **mac-rewrite** configuration. [PR1189353](#)
- The I2C log error message is printed. [PR1251604](#)
- EX3400 Virtual Chassis has tail drops on multicast queues due to incorrect shared buffer programming. [PR1269326](#)
- Traffic loss might be observed for about 10 seconds if the master member FPC reboots. [PR1283702](#)
- Doing load replace terminal and attempting to replace the interface stanza might terminate the current CLI session and leave the user session hanging. [PR1293587](#)
- Some packets might be dropped after GRE encapsulation on EX4300. [PR1293787](#)
- Syslogs contain messages with **%PFE-3: fpc0 ifd null, port 28 dc-pfe: %USER-3: ifd null, port 28 : %PFE-3: fpc0 ifd null, port 29 dc-pfe: %USER-3: ifd null, port 29**. [PR1295711](#)
- Eswd core file might be observed if **apply-groups** is configured under **interface-range**. [PR1300709](#)
- On EX4300 switches, when unknown unicast ICMP packets are received by an interface, packets are routed, so TTL is decremented. [PR1302070](#)
- Unknown IPv6 multicast traffic are dropped if mld-snooping is enabled. [PR1304345](#)
- The **show snmp mib walk** CLI command used for jnxMIMstMstiPortState does not display anything in Junos OS Release 17.1R2 on the EX4600 platform. [PR1305281](#)
- On EX2300 and EX3400 Virtual Chassis or standalone chassis, IP routing fails for destination routes (IPv4 or IPv6 routes) with prefix length of 32 or 128 when they point to ECMP nexthops. [PR1305462](#)
- Inconsistent IEEE P-bit marking occurs in 802.1Q header for OSPF packets. [PR1306750](#)
- The me0 link might stay up after the link is disabled. [PR1307085](#)
- Multicast receiver connected to EX4300 might not be able to get the multicast streaming. [PR1308269](#)
- Multicast receiver connected to EX4300 might not be able to receive the multicast streaming. [PR1308269](#)
- VLAN rewrite is not working on aggregated Ethernet interface for EX2300/3400. [PR1309998](#)

- Traceroute is not working in EX9200 device for routing instances running on Junos OS Release 17.1R3. [PR1310615](#)
- Traffic loss is observed while performing NSSU. [PR1311977](#)
- IGMP snooping might not learn multicast router interface dynamically. [PR1312128](#)
- The DHCP security binding table might not get updated. [PR1312670](#)
- The PoE-enabled port does not come up after reboot of the line card member in EX3400 Virtual Chassis. [PR1312983](#)
- A memory leak is seen for dot1xd. [PR1313578](#)
- The interface with 1G SFP might go down if **no-auto-negotiation** is configured. [PR1315668](#)
- Policer does not work for 224.0.0.X MC traffic to the kernel on EX4300s. [PR1313251](#)
- On EX2300 and EX3400 switches, access ports might incorrectly send VLAN-tagged traffic. [PR1315206](#)
- Need to replace the **show vlans evpn** command with the **show ethernet-switching evpn** command for EX92xx and QFX Series switches. [PR1316272](#)
- Image upgrade fails with the error message **ERROR: Failed to add Junos-**. [PR1317425](#)
- EX2300 interface statistics shows an incorrect bits-per-second (bps) value when the interface has line-rate traffic at 10 Gbps. [PR1318767](#)
- L2cpd core files might be seen if the interface is disabled under VSTP and enabled under RSTP. [PR1317908](#)
- A vmcore file 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 the other FPC. [PR1319795](#)
- EX3400 changes FAN speed frequently with Over Temperature alarm after a software upgrade. [PR1320687](#)
- VLAN might not be processed, which leads to improper STP convergence. [PR1320719](#)
- On the EX2300-48 platform, known unicast might be flooded if the source MAC address is on PFE1 and the destination MAC address is on PFE0. [PR1321612](#)
- Multicast traffic might not be forwarded to one of the receivers. [PR1323499](#)
- EX3400: MACsec not supported on 10G uplink ports. [PR1325545](#)
- L2cpd might create a core file. [PR1325917](#)
- EX Series switches do not send RADIUS request after modifying the interface-range configuration. [PR1326442](#)
- Packets with the DEI bit set in the L2 header are not forwarded on the EX3400 switches. [PR1326855](#)
- EX4600, QFX5100, and ACX5000: Major Alarm **Fan & PSU Airflow direction mismatch** is seen after removing the management cable. [PR1327561](#)

- DHCP packet duplication issue is seen on EX2300/EX3400. [PR1326857](#)
- New operational status detail command is added in **show poe** interface. [PR1330183](#)
- EX3400 CPU have hog when Continuous Telnet EC command are sent on more than 75 concurrent telnet session. [PR1331234](#)
- IP Directed broadcast traffic forwarding does not work on EX3400/EX2300 platform. Applications such as Wakeup-on-lan do not work without this support. [PR1331326](#)
- EX3400 floods unicast ARP replies when DAI is enabled. [PR1331928](#)
- EX2300-48T: "Base power reserved" value seen is higher than "Total power supplied" in **show chassis power-budget-statistics** command. [PR1333032](#)
- Group unknown is seen on **show filter hw 1 show_term_info** CLI after adding **tcam-group-optimization** CLI. [PR1333367](#)
- EX9200 -- Major Errors - MQSS Error code: 0x2203cb. [PR1334928](#)
- IGMP traffic going out of RTG backup link is causing a loop. [PR1335733](#)
- VLAN rewrite might not work properly on trunk ports. [PR1336174](#)

Routing Protocols

- An mcsnoopd core file is seen at **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](#)

User Interface and Configuration

- EX2300 Virtual Chassis committing from J-Web causes PHP process to spike high. [PR1328323](#)

SEE ALSO

[New and Changed Features | 19](#)

[Changes in Behavior and Syntax | 27](#)

[Known Behavior | 30](#)

[Known Issues | 31](#)

[Documentation Updates | 41](#)

[Migration, Upgrade, and Downgrade Instructions | 42](#)

[Product Compatibility | 43](#)

Documentation Updates

IN THIS SECTION

- [New Simplified Documentation Architecture | 41](#)

This section lists the errata and changes in Junos OS Release 18.1R2 for the EX Series switches documentation.

New Simplified Documentation Architecture

- With the release of Junos OS Release 18.1, Juniper is simplifying its technical documentation to make it easier for you to find information and know that you can rely on it when you find it. In the past, we organized documentation about Junos OS software features into platform-specific documents. In many cases, features are supported on multiple platforms, so you might not easily find the document you want for your platform.

With Junos OS Release 18.1, we have eliminated the platform-specific software feature documents. For example, if you want to find documentation on OSPF, there is only one document regardless of which platform you have. Here are some of the benefits of our new simplified architecture:

- Over time, you will see better search results when looking for Juniper documentation. You will be able to find what you want faster and be assured that is the right document.
- If a software feature is supported on multiple platforms, you can find information about all the platforms in one place.
- Because we have eliminated many documents that covered similar topics, you will now find one document with all the information.
- You can know that you are always getting the most current and accurate information.

SEE ALSO

[New and Changed Features | 19](#)

[Changes in Behavior and Syntax | 27](#)

[Known Behavior | 30](#)

[Known Issues | 31](#)

[Resolved Issues | 35](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 42](#)

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](#).

NOTE:

- : EX2300 or EX3400 switches running Junos OS Software Release 15.1X53-D57 or earlier revisions cannot be directly upgraded via CLI to Junos OS Software Release 18.1R1 because of configuration incompatibilities between the two releases related to the uplink port configurations. For example: Any configuration having interfaces on the uplink module (xe-0/2/*) will throw errors during the upgrade process. To work around this problem, please specify the validate option in the upgrade command to check for these errors, then remove the configuration that results in the errors, and use the no-validate option to do the upgrade.

Alternately, an intermediate upgrade to 15.1X53-D58 can be performed by keeping the configuration intact and then a subsequent upgrade to 18.1R1 is possible.
- NSSU is not supported on EX2300-VC/EX3400-VC from Junos OS Release 15.1X53 to Junos OS Release 18.1R1 or later releases. For example, NSSU is not supported from Junos OS Release 15.1X53-D58 to Junos OS Release 18.1R1 or Junos OS Release 15.1X53-D57 to Junos OS Release 18.2R1.

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 17.1, 17.2 and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

SEE ALSO

New and Changed Features 19
Changes in Behavior and Syntax 27
Known Behavior 30
Known Issues 31
Resolved Issues 35
Documentation Updates 41
Product Compatibility 43

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 43](#)

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 19
Changes in Behavior and Syntax 27
Known Behavior 30
Known Issues 31
Resolved Issues 35
Documentation Updates 41
Migration, Upgrade, and Downgrade Instructions 42

Junos OS Release Notes for Junos Fusion Data Center

IN THIS SECTION

●	New and Changed Features 45
●	Changes in Behavior and Syntax 49
●	Known Behavior 49
●	Known Issues 50
●	Resolved Issues 51
●	Documentation Updates 52
●	Migration, Upgrade, and Downgrade Instructions 53
●	Product Compatibility 60

These release notes accompany Junos OS Release 18.1R2 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/software/junos/>

New and Changed Features

IN THIS SECTION

- [Junos Fusion Data Center | 45](#)

This section describes the new features and enhancements to existing features in Junos OS Release 18.1R2 for Junos Fusion Data Center.

Junos Fusion Data Center

- **Junos Fusion Data Center with four aggregation devices and EVPN infrastructure (Junos Fusion Data Center)**—Starting with Junos OS Release 18.1R2-S2, Junos Fusion Data Center supports four aggregation devices to which each satellite device can be multihomed in active-active mode. In this topology, the four aggregation devices comprise a core fabric in which Ethernet VPN (EVPN) is implemented as the control plane in which host and server MAC addresses, network reachability, and other states learned by an aggregation device are advertised to the other aggregation devices. For the data plane, the aggregation devices use Virtual Extensible LAN (VXLAN) encapsulation when forwarding a Layer 2 data packet to other aggregation devices. Namely, an aggregation device encapsulates a data packet in a VXLAN UDP header and sends the packet by means of the Layer 3 network to another aggregation device. Upon receipt of the packet, the aggregation device de-encapsulates the packet and forwards it as appropriate.

Junos Fusion Data Center with four aggregation devices and an EVPN architecture implements IEEE 802.1BR processing between the aggregation devices and satellite devices.

[See [Understanding EVPN in a Junos Fusion Data Center.](#)]

- **Layer 2 unicast forwarding on extended ports (Junos Fusion Data Center)**—Starting with Junos OS Release 18.1R2-S2, Junos Fusion Data Center supports Layer 2 unicast forwarding on extended ports. When a remote MAC address is learned from a Type-2 MAC route advertisement, the aggregation device determines the corresponding extended port next hop from the Ethernet Segment Identifier (ESI) carried in the MAC route advertisement. This extended port next hop is resolved in the set of local cascade interfaces that are used to reach that extended port. Traffic sent to a destination extended port only traverses the EVPN tunnel if the destination extended port cannot be resolved to a local cascade interface. For non-extended port destinations located on a remote aggregation device (or external Provider Edge

(PE) device in the same EVPN), traffic is carried in the EVPN tunnel. When EVPN MAC aliasing is enabled, aggregation devices signal their reachability towards the destination extended port using the per-EVI Ethernet A-D route, so that a list of aggregation devices can be built for load-balancing even if those aggregation devices have not advertised that specific MAC route.

[See [Understanding EVPN in a Junos Fusion Data Center](#).]

- **Layer 2 multicast support with local replication in an EVPN topology (Junos Fusion Data Center)**—Starting with Junos OS Release 18.1R2-S2, Junos Fusion Data Center with EVPN combines elements of an EVPN multicast infrastructure with 802.1BR local replication to support Layer 2 multicast forwarding. In this environment, each extended port on a satellite device is multihomed to all aggregation devices and modeled as an EVPN Ethernet Segment (ES). One aggregation device is elected as the designated forwarder (DF) for each ES (based on the extended port's satellite device DF), and the IGMP snooping state is synchronized on all aggregation devices connected to that ES for faster convergence when DF re-election is required.

To forward multicast traffic, a source aggregation device employs local bias forwarding towards any locally reachable extended port multicast destinations, and uses ingress replication to the other aggregation devices in the EVPN/VxLAN tunnel acting as DFs for other ES destinations. Any forwarding aggregation device also uses 802.1BR local replication to destination satellite devices if you configure the **local-replication** statement at the `[edit forwarding-options satellite]` hierarchy level. Local replication, also referred to as egress replication at the satellite devices, helps distribute packet replication load and reduce traffic on cascade ports for multicast traffic by having the forwarding aggregation device send only one copy of a packet to each satellite device that has an extended port in the multicast group, and the satellite device then does the replication for its local extended ports.

- **Layer 3 multicast support in an EVPN topology (Junos Fusion Data Center)**—Starting with Junos OS Release 18.1R2-S2, Junos Fusion Data Center with EVPN includes support for sending Layer 3 multicast traffic between two extended ports, or link aggregation of extended ports, located in different VLANs. Participating servers can be connected to the fabric through the same tenant. Or they can be connected via different tenants, in which case traffic must transit an external gateway (so the gateway can handle the routing between tenants).

In the EVPN topology, two or more satellite devices (SDs) are multihomed to four QFX10K aggregation devices (ADs), and a multicast VLAN is provisioned between the ADs and the external gateways. When connected to the SD, both the source and receiver ports can be inside the fabric. Or, one can be external to the fabric while the other is internal. Instead of running PIM on the ADs, IGMP reports are sent to the gateways in order to pull traffic from an external source.

- **Configuration synchronization for up to four aggregation devices (Junos Fusion Data Center)**—Starting in Junos OS Release 18.1R2-S2, configuration synchronization enables you to easily propagate, synchronize, and commit configurations from one aggregation device (AD) to another AD. Log in to either AD to manage the other three ADs, and use configuration groups to simplify the configuration process. You can create one configuration group each for the local ADs, and a global configuration common to all ADs.

Create conditional groups to specify when configurations are synchronized. Enable peers-synchronize at the **[edit system commit]** hierarchy to synchronize configurations and commits across ADs by default. NETCONF over SSH provides a secure connection between ADs. Secure Copy Protocol (SCP) copies configurations securely between them.

[See [Understanding Multichassis Link Aggregation Group Configuration Consistency Check.](#)]

- **Satellite device support (QFX5110 and QFX5200)**—Starting with Junos OS Release 18.1R2-S2, you can configure QFX5110-48S and QFX5200-32C switches as satellite devices in a Junos Fusion Data Center topology. The satellite device in a Junos Fusion topology is managed and configured by the aggregation device. Junos Fusion Data Center uses QFX10002, QFX10008 and QFX10016 switches in the aggregation device role.

[See [Junos Fusion Data Center Software and Hardware Requirements.](#)]

- **Flow-based uplink selection (Junos Fusion Data Center)**—Starting in Junos OS Release 18.1R2-S2, you can configure flow-based uplink selection for satellite devices by defining a chassis group to which the uplink traffic flows will be directed.

[See [Understanding Remapping Uplink Traffic Flows on a Junos Fusion Data Center.](#)]

- **Increased number of aggregated Ethernet interfaces (Junos Fusion Data Center)**—Starting in Junos OS Release 18.1R2-S2, you can configure up to 1750 aggregated Ethernet interfaces for a Junos Fusion Data Center system. 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.

[See [Understanding Link Aggregation and Link Aggregation Control Protocol in a Junos Fusion.](#)]

- **Class of service support (Junos Fusion Data Center)**—Starting in Junos OS Release 18.1R2-S2, Junos Fusion Data Center supports the standard Junos class of service (CoS) features and operational commands in a quad-aggregation device configuration. Each extended port on a satellite device is a logical extension to the aggregation device. Therefore, the default CoS policy on the aggregation device applies to each extended port. You can also create standard CoS policies for extended ports.

A cascade port is a physical port or interface on an aggregation device that provides a connection to a satellite device. Port scheduling is supported on cascade ports. Junos Fusion technology reserves a separate set of queues with minimum bandwidth guarantees for in-band management traffic to protect against congestion caused by data traffic.

[See [Understanding CoS in Junos Fusion Data Center.](#)]

- **VLAN flooding support with local replication in an EVPN topology (Junos Fusion Data Center)**—Starting with Junos OS Release 18.1R2-S2, Junos Fusion Data Center with EVPN combines elements of an EVPN multicast infrastructure with 802.1BR local replication to support Layer 2 VLAN flooding. Local replication helps distribute packet replication load and reduce traffic on cascade ports for multicast and flooded VLAN traffic. In this environment, each extended port on a satellite device is multi-homed to all aggregation devices and modeled as an EVPN Ethernet Segment (ES). One aggregation device is elected as the designated forwarder (DF) for each ES (based on the extended port's satellite device DF).

An aggregation device might initiate VLAN flooding (broadcasting or flooding the packet out to all interfaces in the VLAN) to learn the MAC address for a destination that is not already in its Ethernet switching tables. With local replication enabled, the aggregation device requests multicast ECIDs to represent the extended ports in the VLAN on each satellite device. You configure 802.1BR local replication to destination satellite devices by configuring the **local-replication** statement at the **[edit forwarding-options satellite]** hierarchy level.

- **Support for designated trap forwarding of SNMP traps in an EVPN topology (Junos Fusion Data Center)**—Starting with Junos OS Release 18.1R2-S2, you can enable SNMP on the aggregation device and designate trap forwarding in an EVPN topology in Junos Fusion Data Center. In an EVPN topology, the satellite device generates an SNMP trap event when a change occurs on any of the associated satellite devices. This trap event information is sent to all connected aggregation devices who then sends the trap request to the SNMP server. Because each aggregation devices sends its own copy of the trap, the SNMP server receives multiple copies of the trap for the same event on the satellite device, thereby causing overhead to the SNMP server. To prevent the trap from being generated for each aggregation device, you can enable designated trap forwarding so that the trap request is only sent by the aggregation device selected as the designated router. You enable designate trap forwarding under the **[satellite-management]** hierarchy. Designated event forwarding is disabled by default.

[See [Understanding Junos Fusion Data Center With EVPN.](#)]

- **Storm control on extended ports (Junos Fusion Data Center)**—Starting in Junos OS Release 18.1R2-S2, storm control is supported on the extended ports of the satellite device in a Junos Fusion Data Center. You can configure storm control from the aggregation device to rate-limit broadcast traffic, multicast traffic, and unknown unicast traffic level so that the fabric drops packets when the specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN. You specify the storm control level as the traffic rate in kilobits per second (Kbps) of the combined traffic streams, or as the percentage of available link bandwidth used by the combined traffic streams. If the storm control is exceeded, you can also configure the extended ports to shut down interfaces by using the **action-shutdown** command, or by temporarily disabling the interfaces by using the **port-error-disable** command. Additionally, you can disable storm control on registered or unregistered multicast traffic.

[See [Understanding Storm Control.](#)]

- **Firewall filter support on extended ports (Junos Fusion Data Center)**—Starting in Junos OS Release 18.1R2-S2, you can configure firewall filters on extended ports in a Junos Fusion Data Center. An extended port is a physical interface on the satellite device that is managed through the aggregation device. From the aggregation device, you can configure a firewall filter to accept or discard a packet before it enters or exits the port. If a packet is accepted, you can configure additional actions to perform on the packet, such as class-of-service (CoS) marking (grouping similar types of traffic together and treating each type of traffic as a class with its own level of service priority) and traffic policing (controlling the maximum rate of traffic sent or received). To use a firewall filter, you must first configure the filter and then apply it to the port. Firewall filters are defined under the **[edit firewall]** hierarchy level. This feature was previously supported in an "X" release of Junos OS.

[See [Overview of Firewall Filters.](#)]

SEE ALSO

Changes in Behavior and Syntax 49
Known Behavior 49
Known Issues 50
Resolved Issues 51
Documentation Updates 52
Migration, Upgrade, and Downgrade Instructions 53
Product Compatibility 60

Changes in Behavior and Syntax

There are no changes in behavior and syntax for Junos Fusion Data Center in Junos OS Release 18.1R2.

SEE ALSO

New and Changed Features 45
Known Behavior 49
Known Issues 50
Resolved Issues 51
Documentation Updates 52
Migration, Upgrade, and Downgrade Instructions 53
Product Compatibility 60

Known Behavior

IN THIS SECTION

- [Junos Fusion Data Center | 50](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.1R2 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

- In a Junos Fusion Data Center, auto-channelization is not supported on 100G interfaces. As a workaround, you can set the channelization using the **channel-speed** CLI statement at the **[edit policy-options satellite-policies extended-ports-template *template-name* pic *pic-number* port *port-number*]** hierarchy level.

SEE ALSO

New and Changed Features 45
Changes in Behavior and Syntax 49
Known Issues 50
Resolved Issues 51
Documentation Updates 52
Migration, Upgrade, and Downgrade Instructions 53
Product Compatibility 60

Known Issues

There are no known issues in hardware and software in Junos OS Release 18.1R2 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 45
Changes in Behavior and Syntax 49
Known Behavior 49

[Resolved Issues | 51](#)

[Documentation Updates | 52](#)

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

[Product Compatibility | 60](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 18.1R2 | 51](#)

- [Resolved Issues: 18.1R1 | 51](#)

This section lists the issues fixed in the Junos OS Release 18.1R2 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.

Resolved Issues: 18.1R2

Junos Fusion Data Center

- On a Junos Fusion topology with QFX10002 switches as aggregate devices having dual cascade links to each satellite devices for redundancy, duplicated multicast traffic might be seen on downstream devices and multicast receivers if the multicast traffic passes through the aggregate devices. As a workaround, deactivate and re-activate the VLAN in which duplicated multicast traffic is seen. [PR1316499](#)
- In a Junos Fusion setup, an aggregate device may show a plus sign on the ICL link for a satellite device. [PR1335373](#)

Resolved Issues: 18.1R1

Junos Fusion Data Center

- 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](#)

SEE ALSO

New and Changed Features 45
Changes in Behavior and Syntax 49
Known Behavior 49
Known Issues 50
Documentation Updates 52
Migration, Upgrade, and Downgrade Instructions 53
Product Compatibility 60

Documentation Updates

This section lists the errata or changes in Junos OS Release 18.1R2 for Junos Fusion Data Center documentation.

New Simplified Documentation Architecture

- With the release of Junos OS Release 18.1, Juniper is simplifying its technical documentation to make it easier for you to find information and know that you can rely on it when you find it. In the past, we organized documentation about Junos OS software features into platform-specific documents. In many cases, features are supported on multiple platforms, so you might not easily find the document you want for your platform.

With Junos OS Release 18.1, we have eliminated the platform-specific software feature documents. For example, if you want to find documentation on OSPF, there is only one document regardless of which platform you have. Here are some of the benefits of our new simplified architecture:

- Over time, you will see better search results when looking for Juniper documentation. You will be able to find what you want faster and be assured that is the right document.
- If a software feature is supported on multiple platforms, you can find information about all the platforms in one place.
- Because we have eliminated many documents that covered similar topics, you will now find one document with all the information.
- You can know that you are always getting the most current and accurate information.

SEE ALSO

New and Changed Features 45
Changes in Behavior and Syntax 49

Known Behavior	49
Known Issues	50
Resolved Issues	51
Migration, Upgrade, and Downgrade Instructions	53
Product Compatibility	60

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Basic Procedure for Upgrading an Aggregation Device | 53
- Preparing the Switch for Satellite Device Conversion | 55
- Configuring Satellite Device Upgrade Groups | 57
- Converting a Satellite Device to a Standalone Device | 58
- Upgrade and Downgrade Support Policy for Junos OS Releases | 59
- Downgrading from Junos OS Release 18.1 | 59

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 **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](#).

To download and install Junos OS:

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/>
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology > Junos Platform > Junos Fusion** to find the software that you want to download.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list 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.

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

All other customers, use the following command.

```
user@host> request system software add 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 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 hardware and software requirements, see [Junos Fusion Hardware and Software Compatibility Matrices](#).

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

- The 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, replacing *n* with the spin number:

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

Customers with QFX5100 switches, use the following command, replacing *n* with the spin number:

```
user@host> request system software add validate reboot
source/jinstall-qfx-5-14.1X53-D43.n-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:

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

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

If you are not logged in to the device using the console port connection, your connection to the device is lost after 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. See [Configuring or Expanding a Junos Fusion Data Center](#) for detailed configuration steps for each method.

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*** 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/package-name
```

NOTE: Before issuing **request system software add upgrade-group *group-name***, 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. For more information, see [Converting a Satellite Device to a Standalone Device](#).

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 17.1, 17.2 and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or even from Junos OS Release 17.1 to Release 17.3.

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

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

Downgrading from Junos OS Release 18.1

To downgrade from Junos OS Release 18.1 to another supported release, follow the procedure for upgrading, but replace the 18.1 **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 | 45](#)

[Changes in Behavior and Syntax | 49](#)

[Known Behavior | 49](#)

[Known Issues | 50](#)

[Resolved Issues | 51](#)

[Documentation Updates | 52](#)

[Product Compatibility | 60](#)

Product Compatibility

IN THIS SECTION

- [Hardware and Software Compatibility | 60](#)
- [Hardware Compatibility Tool | 60](#)

Hardware and Software Compatibility

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

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 in a Junos Fusion, 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 45
Changes in Behavior and Syntax 49
Known Behavior 49
Known Issues 50
Resolved Issues 51
Documentation Updates 52
Migration, Upgrade, and Downgrade Instructions 53

Junos OS Release Notes for Junos Fusion Enterprise

IN THIS SECTION

- New and Changed Features | 61
- Changes in Behavior and Syntax | 62
- Known Behavior | 63
- Known Issues | 63
- Resolved Issues | 64
- Documentation Updates | 66
- Migration, Upgrade, and Downgrade Instructions | 67
- Product Compatibility | 72

These release notes accompany Junos OS Release 18.1R2 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/software/junos/>.

New and Changed Features

IN THIS SECTION

- Junos Fusion Enterprise | 62

This section describes the new features and enhancements to existing features in Junos OS Release 18.1R2 for Junos Fusion Enterprise.

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

Junos Fusion Enterprise

Junos Fusion Enterprise

- **Aggregation device support on EX9251 switches (Junos Fusion Enterprise)**—Starting with Junos OS Release 18.1R1, EX9251 switches are supported as aggregation devices in a Junos Fusion Enterprise. The aggregation device acts as the single point of management for all devices in the Junos Fusion Enterprise. Junos Fusion Enterprise supports the 802.1BR standard.

[See [Junos Fusion Enterprise Overview](#).]

SEE ALSO

Changes in Behavior and Syntax 62
Known Behavior 63
Known Issues 63
Resolved Issues 64
Documentation Updates 66
Migration, Upgrade, and Downgrade Instructions 67
Product Compatibility 72

Changes in Behavior and Syntax

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 18.1R2 for Junos Fusion Enterprise.

SEE ALSO

New and Changed Features 61

Known Behavior	 63
Known Issues	 63
Resolved Issues	 64
Documentation Updates	 66
Migration, Upgrade, and Downgrade Instructions	 67
Product Compatibility	 72

Known Behavior

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 18.1R2 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.

SEE ALSO

New and Changed Features	 61
Changes in Behavior and Syntax	 62
Known Issues	 63
Resolved Issues	 64
Documentation Updates	 66
Migration, Upgrade, and Downgrade Instructions	 67
Product Compatibility	 72

Known Issues

IN THIS SECTION

- [Junos Fusion Enterprise](#) | 64

This section lists the known issues in hardware and software in Junos OS Release 18.1R2 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 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](#)
- In a Junos Fusion Enterprise, it could take 6 to 30 seconds for the traffic to converge when on the aggregation device is powered **OFF** or powered **ON**. [PR1257057](#)
- In a Junos Fusion Enterprise, during RE switchover, the BUM traffic is duplicated to indirectly connected satellite devices. This is because there is no current support to notify the GRES event to indirectly connected satellite devices. [PR1298434](#)

SEE ALSO

New and Changed Features	 61
Changes in Behavior and Syntax	 62
Known Behavior	 63
Resolved Issues	 64
Documentation Updates	 66
Migration, Upgrade, and Downgrade Instructions	 67
Product Compatibility	 72

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 18.1R2](#) | [65](#)
- [Resolved Issues: 18.1R1](#) | [65](#)

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: 18.1R2

Junos Fusion Enterprise

- In a Junos Fusion Enterprise in which port mirroring analyzers are configured, mirrored packets are dropped when the packets must traverse the interchassis link (ICL) link to reach destination extended ports. As a workaround, you can alternatively configure a remote switched port analyzer (RSPAN) VLAN with the extended ports and the ICL link as members and configure the RSPAN VLAN as the analyzer destination. [PR1211123](#)
- In a Junos Fusion setup, an aggregate device may show a plus sign on the ICL link for a satellite device. [PR1335373](#)
- Issue with 802.1X re-authentication in Junos Fusion Enterprise. [PR1345365](#)

Resolved Issues: 18.1R1

Junos Fusion Enterprise

- Request chassis satellite beacon functionality to specific satellite device is not working, causing all the satellite devices to enable the beacon LED. [PR1272956](#)
- 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. [PR1275290](#)
- Junos Fusion : SD EX4300 displaying U-Boot on LCD screen. [PR1304784](#)
- All 802.1X authentication sessions are removed when the AUTO ICCP link is disabled. [PR1307588](#)
- LACP aggregated Ethernet interfaces go to down state when performing **commit synchronize**. [PR1314561](#)
- Packets loss for 2-3 seconds is seen in every 5 minutes on Junos Fusion. [PR1320254](#)
- In a Junos Fusion Enterprise deployment, an SCPD core might be seen on an aggregation device when DACL on dot1x enabled port is installed on a single homed satellite device.. [PR1328247](#)
- When the ICCP and IFBDs are in transition--Down/Up--DHCP security binding entries might be missing from server database. [PR1332828](#)

SEE ALSO

New and Changed Features 61
Changes in Behavior and Syntax 62
Known Behavior 63
Known Issues 63
Documentation Updates 66
Migration, Upgrade, and Downgrade Instructions 67
Product Compatibility 72

Documentation Updates

This section lists the errata and changes in Junos OS Release 18.1R2 documentation for Junos Fusion.

New Simplified Documentation Architecture

- With the release of Junos OS Release 18.1, Juniper is simplifying its technical documentation to make it easier for you to find information and know that you can rely on it when you find it. In the past, we organized documentation about Junos OS software features into platform-specific documents. In many cases, features are supported on multiple platforms, so you might not easily find the document you want for your platform.

With Junos OS Release 18.1, we have eliminated the platform-specific software feature documents. For example, if you want to find documentation on OSPF, there is only one document regardless of which platform you have. Here are some of the benefits of our new simplified architecture:

- Over time, you will see better search results when looking for Juniper documentation. You will be able to find what you want faster and be assured that is the right document.
- If a software feature is supported on multiple platforms, you can find information about all the platforms in one place.
- Because we have eliminated many documents that covered similar topics, you will now find one document with all the information.
- You can know that you are always getting the most current and accurate information.

SEE ALSO

New and Changed Features 61
Changes in Behavior and Syntax 62

[Known Behavior | 63](#)[Known Issues | 63](#)[Resolved Issues | 64](#)[Migration, Upgrade, and Downgrade Instructions | 67](#)[Product Compatibility | 72](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading Junos OS on an Aggregation Device | 67](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 69](#)
- [Preparing the Switch for Satellite Device Conversion | 70](#)
- [Converting a Satellite Device to a Standalone Switch | 71](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 71](#)
- [Downgrading from Junos OS Release 18.1 | 72](#)

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 18.1R2:

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/>
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology > Junos Platform > Junos Fusion** to find the software that you want to download.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list on the right of the page.
5. Select the **Software** tab.
6. Select the software package for the release.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **junos-install** package on the aggregation device.

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

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

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

All other customers, use the following command:

```
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 Canada and U.S. version)

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

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

Rebooting occurs only if the upgrade is successful.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

For the detailed procedure, see the [Installation and Upgrade Guide](#).

Preparing the Switch for Satellite Device Conversion

There are multiple methods to upgrade or downgrade satellite software in your Junos Fusion 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: The following conditions must be met before a Junos switch that is running Junos OS Release 14.1X53-D43 can be converted to a satellite device when the action is initiated from the aggregation device:

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

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

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

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

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

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

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

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

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

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

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, or preconfiguration. See [Configuring or Expanding a Junos Fusion 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 it from the Junos Fusion topology. For more information, see [Converting a Satellite Device to a Standalone Device](#).

Upgrade and Downgrade Support Policy for Junos OS Releases

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 17.1, 17.2 and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

Downgrading from Junos OS Release 18.1

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.

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

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

SEE ALSO

[New and Changed Features | 61](#)

[Changes in Behavior and Syntax | 62](#)

[Known Behavior | 63](#)

[Known Issues | 63](#)

[Resolved Issues | 64](#)

[Documentation Updates | 66](#)

[Product Compatibility | 72](#)

Product Compatibility

IN THIS SECTION

● [Hardware and Software Compatibility | 73](#)

● [Hardware Compatibility Tool | 73](#)

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 in a Junos Fusion, 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	 61
Changes in Behavior and Syntax	 62
Known Behavior	 63
Known Issues	 63
Resolved Issues	 64
Documentation Updates	 66
Migration, Upgrade, and Downgrade Instructions	 67

Junos OS Release Notes for Junos Fusion Provider Edge

IN THIS SECTION

- New and Changed Features | 74
- Changes in Behavior and Syntax | 76
- Known Behavior | 77
- Known Issues | 78
- Resolved Issues | 80
- Documentation Updates | 81
- Migration, Upgrade, and Downgrade Instructions | 82
- Product Compatibility | 89

These release notes accompany Junos OS Release 18.1R2 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/software/junos/>.

New and Changed Features

IN THIS SECTION

- Release 18.1R2 New and Changed Features | 75
- Release 18.1R1 New and Changed Features | 75

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 18.1R2 New and Changed Features

There are no new features or enhancements to existing features for Junos Fusion Provider Edge in Junos OS Release 18.1R2.

Release 18.1R1 New and Changed Features

Hardware

- **Support for QFX5110 and QFX5200 as satellite devices in Junos Fusion Provider Edge**—Starting in Junos OS Release 18.1R1, you can use QFX5110-48S or QFX5200-32C switches as satellite devices in Junos Fusion Provider Edge.

[See [Satellite Device Hardware Models](#) and [Preparing the Satellite Device](#).]

Class of Service (CoS)

- **Support for dynamic mapping of extend ports to cascade ports for hierarchical CoS (Junos Fusion Provider Edge)**—Junos Fusion treats the cascade ports connecting the aggregation device to the satellite device as aggregated Ethernet ports with aggregation done automatically without configuration. By default the Junos Fusion implementation of hierarchical CoS applies the scheduler parameters across all cascade ports in **scale** mode. Because **scale** mode divides the configured shaper equally across the cascade ports, traffic drops can start before a customer reaches its committed rate for a particular flow. To avoid this problem, starting with Junos OS Release 18.1R1, you can set all cascade ports on an aggregation device to be in **replicate** mode and automatically target all of a customer's traffic to a specific cascade port. To do this, simply enable **target-mode** at the **[edit chassis satellite-management fpc-number]** hierarchy level.

[See [Understanding CoS on an MX Series Aggregation Device in Junos Fusion](#).]

Junos Fusion

- **Junos Fusion Provider Edge support for Junos Node Slicing (MX960, MX2010, MX2020)**—Starting in Junos OS Release 18.1R1, you can configure an aggregation device on guest network functions (GNFs), or partitions created on a router, by using Junos Node Slicing. The Junos Fusion topology is composed of an aggregation device and multiple satellite devices. An MX Series router supports a maximum of 10 GNFs, with each GNF supporting a separate aggregation device. The aggregation device on a GNF supports a maximum of 10 satellite devices. The aggregation device acts as the single point of management for all devices in a Junos Fusion topology, while the satellite devices provide interfaces that send and receive network traffic.

For more information on Junos Node Slicing, see [Junos Node Slicing Overview](#).

NOTE:

- In a Junos Fusion Provider Edge topology that has a GNF configured as the aggregation device, you can only use EX4300 switches as satellite devices.
- Only the following line cards support the cascade port on the aggregation device: MPC7, MPC8, or MPC9.

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

SEE ALSO

[Changes in Behavior and Syntax | 76](#)

[Known Behavior | 77](#)

[Known Issues | 78](#)

[Resolved Issues | 80](#)

[Documentation Updates | 81](#)

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

[Product Compatibility | 89](#)

Changes in Behavior and Syntax

There are no changes in default behavior and syntax for Junos Fusion Provider Edge in Junos OS Release 18.1R2.

SEE ALSO

New and Changed Features	74
Known Behavior	77
Known Issues	78
Resolved Issues	80
Documentation Updates	81
Migration, Upgrade, and Downgrade Instructions	82
Product Compatibility	89

Known Behavior

IN THIS SECTION

- Junos Fusion | 77

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.1R2 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.

Junos Fusion

- Configuration synchronization is not triggered when you issue the rollback command on the local aggregation device (AD). [PR1298747](#)
- Configuration synchronization is not triggered when you issue the rollback command on the local aggregation device (AD). [PR1298747](#)
- In Junos OS, two different input filters cannot be configured on the same interface; if two filters are configured, only the second filter (the one that was configured most recently) takes effect. Ingress mirroring on extended ports in Junos Fusion Data Center (JFDC) can only be done by using firewall filters. Considering the Junos OS filter behavior described above, in JFDC, ingress mirroring on extended ports and other firewall filter configurations cannot be done on the same port. [PR1353065](#)
- Since EVPN GR is not supported, restart of rpd will result in considerable traffic loss for EVPN traffic. The traffic should restore eventually once convergence is complete. [PR1353742](#)

SEE ALSO

[New and Changed Features | 74](#)[Changes in Behavior and Syntax | 76](#)[Known Issues | 78](#)[Resolved Issues | 80](#)[Documentation Updates | 81](#)[Migration, Upgrade, and Downgrade Instructions | 82](#)[Product Compatibility | 89](#)

Known Issues

IN THIS SECTION

- [Junos Fusion | 79](#)

This section lists the known issues in hardware and software in Junos OS Release 18.1R2 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.

Junos Fusion

- The license installed will not be deleted, unless it is explicitly deleted using the **request** command. After disabling the cascade port, the license count will be marked as zero only after the satellite information is purged from the neighbor database. Previously this satellite neighbor information persisted for only for 8 minutes; now neighbor information is being held for 8 hours. This time delay is introduced to avoid repeating the initial recognition of the satellite device for interface-down events. **user@host> show configuration | display set | grep et-0/0/30 set groups user-host-grp interfaces et-0/0/30 cascade-port set chassis satellite-management fpc 101 cascade-ports et-0/0/30 set interfaces et-0/0/30 disable {master:0} user@host> show chassis satellite terse**

Device	Extended Ports	Slot	State	Model	Total/Up
Version 100	Online	EX4300-48T 50/1	17.4-20170726_common_xxx.0	102	Online
QFX5200-32C-32Q 2/1	17.4-20170726_common_xxx.0	103	Online	QFX5110-48S-4C 3/2	17.4-20170726_common_xxx.0

{master:0} user@host> show chassis satellite neighbor

Interface	State	Port	Info	System	Name	Model	SW	Version
et-0/0/30	Dn	et-0/0/18	Two-Way	et-0/0/18	sd102	QFX5200-32C-32Q	17.4-20170726_common_xxx.0	et-0/0/12
Two-Way	et-0/0/50	sd103	QFX5110-48S-4C	17.4-20170726_common_xxx.0	et-0/0/6	Two-Way	et-0/1/3	sd100
EX4300-48T	17.4-20170726_common_xxx.0	{master:0}	user@host> show system license	License usage:	Licenses	Licenses	Licenses	Expiry
Feature name	used	installed	needed	bgp 1	0	1	invalid	SD-QFX5100-48SH-48TH
0	4	0	permanent	Licenses installed:	License identifier:	JUNOSxxxxxx	License version:	4
Software	Serial	Number:	99999B99999999	Customer ID:	USER-SWITCH	Features:	SD-QFX5100-48SH-48TH-4PK -	SD 4 pack
QFX5000-10-JFD	permanent	{master:0}	user@host> show system license usage	Licenses	Licenses	Licenses	Licenses	Expiry
Feature name	used	installed	needed	bgp 1	0	1	invalid	SD-QFX5100-48SH-48TH
0	4	0	permanent	{master:0}	user@host> show system alarms	4	alarms	currently active
Alarm time	Class	Description	2017-08-29 13:14:27 UTC	Minor	BGP Routing Protocol usage requires a license	2017-08-28 17:25:27 UTC	Major	FPC0: PEM 1
Not Powered	2017-08-28 17:25:27 UTC	Major	FPC Management	1	Ethernet Link Dow.	PR1294951		
- With IGMP snooping enabled in an EVPN-VXLAN configuration, when a large number of IGMP leaves are received at the same time, some of the leaves might not get processed. As a result, the IGMP group state lingers until it eventually times out on a group membership interval timeout. [PR1327980](#)
- Traffic Drop is seen due to the following reasons: 1) When AD goes down, the routes advertised by that AD are withdrawn causing traffic drop. Centralized or Distributed BFD over VXLAN is not a supported feature on QFX10000 which can improve convergence time. 2) When AD comes up, hold the interface to MX down until AD joins the cluster to minimize traffic getting blackholed (set interfaces <> hold-time up <300 * 1000>). [PR1331465](#)
- On QFX10000, EVPN NSR Unicast will be supported in 18.4 EVPN NSR Multicast support is not scheduled yet and will be tracked via EVPN VXLAN Solution NPI. [PR1337645](#)
- On QFX chassis and fixed platforms, there is high probability during system bring up that kernel modules may be loaded in unexpected order leading to kernel panics. [PR1343075](#)
- Sometimes when some of the EX4300 SDs are rebooted, Under specific conditions there may be logic error included at an internal FIFO. This in turn may lead to corrupted packets entering the packet

processing pipeline in Broadcom. Due to this, sds stay in offline state as lldp packets from Aggregate device ar not handled. [PR1349508](#)

SEE ALSO

New and Changed Features 74
Changes in Behavior and Syntax 76
Known Behavior 77
Resolved Issues 80
Documentation Updates 81
Migration, Upgrade, and Downgrade Instructions 82
Product Compatibility 89

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 18.1R2 | 80](#)
- [Resolved Issues: 18.1R1 | 81](#)

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: 18.1R2

Junos Fusion

- 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](#)

- In a fusion setup, an aggregate device may show 'plus' sign on the ICL link for a satellite device. [PR1335373](#)
- SSH key-based authentication does not work with Junos Fusion. [PR1344392](#)
- AD failure (power off) in a DC fusion is causing complete or partial traffic loss for extended period. [PR1352167](#)

Resolved Issues: 18.1R1

Junos Fusion

- Chassis alarms are not generated after the uplinks are made down from SD. [PR1275480](#)
- The LAG interface might flap if rebooting aggregation device. [PR1315879](#)
- Duplicated packets might be received on the multicast downstream devices and multicast receivers. [PR1316499](#)
- Not able to disable fpc-slot .Getting error Operation not supported for device assigned slot-id. [PR1321268](#)

SEE ALSO

New and Changed Features 74
Changes in Behavior and Syntax 76
Known Behavior 77
Known Issues 78
Documentation Updates 81
Migration, Upgrade, and Downgrade Instructions 82
Product Compatibility 89

Documentation Updates

IN THIS SECTION

- [New Simplified Documentation Architecture | 82](#)

This section lists the errata and changes in Junos OS Release 18.1R2 for Junos Fusion Provider Edge.

New Simplified Documentation Architecture

- With the release of Junos OS Release 18.1, Juniper is simplifying its technical documentation to make it easier for you to find information and know that you can rely on it when you find it. In the past, we organized documentation about Junos OS software features into platform-specific documents. In many cases, features are supported on multiple platforms, so you might not easily find the document you want for your platform.

With Junos OS Release 18.1, we have eliminated the platform-specific software feature documents. For example, if you want to find documentation on OSPF, there is only one document regardless of which platform you have. Here are some of the benefits of our new simplified architecture:

- Over time, you will see better search results when looking for Juniper documentation. You will be able to find what you want faster and be assured that is the right document.
- If a software feature is supported on multiple platforms, you can find information about all the platforms in one place.
- Because we have eliminated many documents that covered similar topics, you will now find one document with all the information.
- You can know that you are always getting the most current and accurate information.

SEE ALSO

[New and Changed Features | 74](#)

[Changes in Behavior and Syntax | 76](#)

[Known Behavior | 77](#)

[Known Issues | 78](#)

[Resolved Issues | 80](#)

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

[Product Compatibility | 89](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading an Aggregation Device | 83](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 85](#)

- [Preparing the Switch for Satellite Device Conversion | 86](#)
- [Converting a Satellite Device to a Standalone Device | 87](#)
- [Upgrading an Aggregation Device | 87](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 87](#)
- [Downgrading from Junos OS Release 18.1 | 88](#)

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 18.1R2 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://www.juniper.net/support/downloads/>
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology > Junos Platform > Junos Fusion** to find the software that you want to download.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list 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 18.1R2 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

For the detailed procedure, see the [Installation and Upgrade Guide](#).

Preparing the Switch for Satellite Device Conversion

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

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

- The switch can only be converted to SNOS 3.1 and higher.
- The 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 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:

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

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

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

If you lose 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 it from the Junos Fusion topology. For more information, see [Converting a Satellite Device to a Standalone Device](#).

Upgrading an Aggregation Device

When you upgrade an aggregation device to Junos OS Release 18.1R2, 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 17.1, 17.2 and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

Downgrading from Junos OS Release 18.1

To downgrade from Junos OS Release 18.1 to another supported release, follow the procedure for upgrading, but replace the 18.1 **jinstall** package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

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

SEE ALSO

[New and Changed Features | 74](#)

[Changes in Behavior and Syntax | 76](#)

[Known Behavior | 77](#)

[Known Issues | 78](#)

[Resolved Issues | 80](#)

[Documentation Updates | 81](#)

[Product Compatibility | 89](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 89](#)

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 in a Junos Fusion, 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 74
Changes in Behavior and Syntax 76
Known Behavior 77
Known Issues 78
Resolved Issues 80
Documentation Updates 81
Migration, Upgrade, and Downgrade Instructions 82

Junos OS Release Notes for MX Series 3D Universal Edge Routers

IN THIS SECTION

- New and Changed Features | 90
- Changes in Behavior and Syntax | 110
- Known Behavior | 115
- Known Issues | 119
- Resolved Issues | 128
- Documentation Updates | 154
- Migration, Upgrade, and Downgrade Instructions | 155
- Product Compatibility | 162

These release notes accompany Junos OS Release 18.1R2 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at <https://www.juniper.net/documentation/software/junos/>.

New and Changed Features

IN THIS SECTION

- Release 18.1R2 New and Changed Features | 91
- Release 18.1R1 New and Changed Features | 91

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 18.1R2 New and Changed Features

Class of Service (CoS)

- **Hierarchical CoS support for anchor point redundancy of pseudowire subscriber logical Interfaces (MX Series)**—Starting in Junos OS Release 18.1R2, full hierarchical CoS support is provided for stateful anchor point redundancy of pseudowire subscriber logical interfaces. 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. Hierarchical CoS is supported and configured the same on both redundant and non-redundant pseudowire subscriber logical interfaces.

[See [CoS Configuration Overview for MPLS Pseudowire Subscriber Interfaces](#).]

Restoration Procedures Failure

- **Device recovery mode introduced in Junos OS with upgraded FreeBSD (MX Series)**—In Junos OS Release 18.1R2, 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](#).]

Software Installation and Upgrade

- **ZTP support is added for MX VM host platforms (MX Series)**—In Junos OS Release 18.1R2, 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](#).]

Release 18.1R1 New and Changed Features

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

- **TACACS+ authorization for operational commands using regular expressions (MX Series)**—Starting in Junos OS Release 18.1R1, you can configure authorizations for operational mode commands using regular expressions using the **allow-commands-regexps** and **deny-commands-regexps** statements. Authorizations can also be configured remotely by specifying Juniper Networks vendor-specific attributes (VSAs) in your TACACS+ authentication server's configuration.

[See [Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies](#).]

Class of Service

- **Support for policer actions before ingress queuing (MX Series)**—Starting with Junos OS Release 18.1R1, on MPCs that support ingress queuing, you can implement policer actions on traffic before the traffic is assigned to ingress queues. To do this, create the desired policers, apply them to a standard firewall filter, and attach the filter as an ingress queuing policing filter [**iq-policing-filter** *filter-name*] to an interface at the [**edit interfaces** *interface-name* **unit** *logical-unit-number* **family** *family*] hierarchy level. The **iq-policing-filter** can only be attached to a static interface.

[See [Ingress Queuing Filter with Policing Functionality](#).]

- **Support for rewrite of the first three bits of IPv6 DSCP value (MX Series, vMX)**—Starting with Junos OS Release 18.1R1, MX Series routers with MPCs support rewrite rules that rewrite only the first three bits of the IPv6 DSCP value. Junos OS provides a new rewrite rule option, **inet6-precedence**, at the [**edit class-of-service** **rewrite-rules**] hierarchy level that allows you to set a 3-bit code point for a particular forwarding class and loss priority for IPv6 traffic. This new rewrite rule option can also be applied to packets entering an MPLS LSP.

[See [inet6-precedence \(CoS Rewrite Rules\)](#).]

Dynamic Host Configuration Protocol (DHCP)

- **DHCP support for management interface in non-default RI (MX Series)**—Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, **mgmt_junos**.

[See [Configuring a DHCP Client](#).]

EVPNs

- **Connectivity Fault Management Support in an EVPN network (MX Series)**—Starting with Junos OS Release 18.1R1, Junos OS supports connectivity fault management (CFM) Up maintenance association endpoints (MEPs) on the attachment circuits (ACs) that are connected to a provider edge (PE) router in an EVPN network. You can configure up MEPs to monitor multiple attachment circuits on the same PE router as part of the same maintenance domain or maintenance association.

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

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

General Routing

- **Support for PTP over Ethernet encapsulation and G.8275.1 profile (MX10003 and MX204)**—Starting in Junos OS Release 18.1R1, MX10003 and MX204 routers support the following features:
 - **PTP over Ethernet**—PTP over Ethernet enables effective implementation of packet-based technology that enables the operator to deliver synchronization services on packet-based mobile backhaul networks. PTP over Ethernet uses multicast addresses for communication of PTP messages between the slave clock and the master clock.
 - **G.8275.1 profile**—G.8275.1 is a PTP profile for applications that require accurate phase and time synchronization. It supports the architecture defined in ITU-T G.8275 to enable the distribution of phase and time with full timing support and is based on the second version of PTP defined in IEEE 1588. You can configure the G.8275.1 profile by including the **profile-type g.8275.1** statement at the **[edit protocols ptp]** hierarchy level.

[See [Configuring G.8275.1 Profile](#).]

- **VRF support for NTP (MX Series)**—Starting in Junos OS Release 18.1R1, NTP clients can send requests to servers that are reachable through VRF. The **set system ntp server address routing-instance routing-instance-name** and **set date ntp routing-instance routing-instance-name** commands let you specify the routing instance that the server can be reached through.

[See [Configuring the NTP Time Server and Time Services](#).]

- **Support for PTP, Synchronous Ethernet, and hybrid mode over link aggregation group (MX240, MX480, MX960, MX2010, MX2020)**—Starting in Junos OS Release 18.1R1, the MPC7E-10G, MPC7E-MRATE, MPC8E, and MPC9E MPCs support Precision Time Protocol (PTP), Synchronous Ethernet, and hybrid mode over a link aggregation group (LAG).

Link aggregation is a mechanism of combining multiple physical links into a single virtual link to achieve linear increase in bandwidth and to provide redundancy in case a link fails. The virtual link is referred to as an aggregated Ethernet interface or a LAG.

[See [Precision Time Protocol Overview](#).]

High Availability and Resiliency

- **MX Series Virtual Chassis Unified ISSU support for MPC7E-10G, MPC7E-MRATE, MPC8E, and MPC9E line cards (MX Series Virtual Chassis)**—Starting in Junos OS Release 18.1R1, MPC7E-10G, MPC7E-MRATE, MPC8E, and MPC9E line cards support Unified ISSU in MX Series Virtual Chassis environments. Unified ISSU enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic.

[See [Unified ISSU in a Virtual Chassis](#).]

Interfaces and Chassis

- **New speed configuration option introduced to change 10-Gbps port to operate in 1-Gbps speed (MX204, MX10003)**—Starting in Junos OS Release 18.1R1, the 10-Gbps port can operate in 1-Gbps mode on MX204 and MX10003 routers. Currently, MX204 and MX10003 routers support different operation modes; that is, 10-Gbps, 40-Gbps, and 100-Gbps speed. When the port is operating in 10-Gbps speed, you can change the operating speed to 1Gbps using a new CLI option, [speed 1g/10g](#) at the **[edit interfaces intf-name together-options]** hierarchy level. Once you commit this configuration, the operating speed of the 10-Gbps port changes to 1-Gbps speed without any FPC, PIC, or interface bounce.

The MX10003 MPC has one fixed PIC and one MIC (non-MACsec MIC/MACsec MIC). The fixed PIC has 6 ports that can operate in 40-Gbps or 4X10-Gbps mode. The MIC has 12 ports that can operate in 100-Gbps, 40-Gbps, or 4X10-Gbps mode. With this new speed configuration option, you can configure the 4X10-Gbps port on the fixed PIC and the non-MACsec MIC to 1-Gbps mode. You can also configure one or all ports that operate in 10-Gbps mode to 1Gbps mode.

The MX204 contains two PICs—where one PIC contains 8 ports that can operate in 10-Gbps mode and the other PIC contains 4 ports that can operate in 4X10-Gbps, 40-Gbps, or 100-Gbps mode. Using this new speed configuration option, you can configure the 4X10-Gbps port on one of the fixed-port PICs to operate in 1-Gbps mode. And on the other fixed-port PIC, you can configure the 10-Gbps port to 1Gbps.

NOTE:

- On the MX10003 router, the MACsec MIC does not provide 1-Gbps speed. If you attempt to change the operating speed to 1-Gbps, syslog displays that this feature is not supported on the MACsec MIC.
- On MX204 and MX10003 routers, rate selectability at PIC level and port level does not support 1-Gbps speed.
- On MX204 and MX10003 routers, 1-Gbps operation mode is only supported in no-autonegotiation mode.

To view the speed configured for the interface, execute the **show interfaces extensive** command. The **Speed Configuration** output parameter in the command output indicates the current operation speed of the interface.

If the interface is configured with 1-Gbps speed, then **Speed Configuration** displays **1G**; if the interface is configured with 10-Gbps speed, **Speed Configuration** displays **AUTO**.

For example:

```
user@host>show interfaces xe-0/1/11:0 extensive
```

```
Physical interface: xe-0/1/11:0, Enabled, Physical link is Up
Interface index: 284, SNMP ifIndex: 609, Generation: 383
Link-level type: Ethernet, MTU: 9192, MRU: 9200, LAN-PHY mode, Speed: 10Gbps,
BPDU Error: None, Loop Detect PDU Error: None, MAC-REWRITE Error: None,
Loopback: None, Source filtering: Disabled, Flow control: Enabled,
Speed Configuration: 1G
...
```

In this example, the **Speed Configuration** output parameter displays **1G**, which means the operation speed of `xe-0/1/11:0` interface is 1-Gbps speed.

NOTE:

- The interface name prefix must be `xe`.
- To set a port that is operating in 10-Gbps speed to 1-Gbps speed, use the new CLI option [speed 1g/10g](#) for the existing **set interfaces [intf-name] gigether-options** command.
- To view the speed configured for the interface, execute the **show interfaces extensive** command.

[See [MX10003 MPC Rate-Selectability Overview](#) and [MX204 Router Rate-Selectability Overview](#).]

- **Upgraded SSD size and RAM size (MX Series)**—Starting in Junos OS Release 18.1R1, the Routing Engines on the MX240, MX480, MX960, MX2010, MX2020 routers support Secure Boot BIOS. The SSD size and the RAM size of the following Routing Engines are upgraded to 2x200-GB and 128-GB respectively:

- RE-S-X6-128G-S on the MX240, MX480, and MX960 routers
- RE-MX2K-X8-128G-S on the MX2010 and MX2020 routers

[See [Salient Features of the Routing Engines with VM Host Support](#).]

- **Limited encryption Junos OS image and boot restriction (MX10003)**—Starting with Junos OS Release 18.1R1, MX10003 router with LT-SKU supports only Junos Limited image. The Junos Limited image does not have data-plane encryption and is intended only for countries in the Eurasian Customs Union because these countries have import restrictions on software containing data plane encryption. Unlike the Junos Worldwide image, the Junos Limited image supports control plane encryption through Secure Shell (SSH) and Secure Sockets Layer (SSL), thus allowing secure management of the system. The MX10003 LT SKU boots only the encryption free Junos software and fails to boot if the fully encrypted Junos software is used for booting. The Junos upgrade and VMHost upgrade using non-limited version of Junos software fails on the MX10003 LT SKU. The command **show chassis hardware [models | clei-models | extensive]** displays the model number and helps identifying the different SKUs. An alarm, **Mixed Master and Backup RE types** is displayed when dissimilar Routing Engines are present on the chassis.

[See [Junos OS Editions](#).]

- **Enhanced support for the non-default management instance mgmt_junos (MX Series)**—Starting in Junos OS Release 18.1R1, syslog IPv6 addresses, RADIUS packets, and Automation scripts support the non-default management instance mgmt_junos, when the **management-instance** statement is configured. For syslog, statements at the **[edit system syslog]** hierarchy level now support IPv6 addresses when connecting to a remote host or an archival site. RADIUS authentication, authorization, and accounting packets can be configured to use the mgmt_junos instance. Also, Automation (commit, event, JET, op, or SNMP) scripts now can be refreshed over the mgmt_junos instance. To enable the non-default VRF management instance, you must also configure the mgmt_junos routing instance at the **[edit system routing-instances]** hierarchy level.

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

- **Enhancement to increase the threshold of corrected single-bit errors (MPC7E, MPC8E, MPC9E on MX Series)**—In Junos OS Release 18.1R1, 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 error detected in HMC 0 - Total count 25

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

[See [Alarm Overview](#).]

- **DHCP support for management interface in non-default RI (MX Series)**—Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, `mgmt_junos`.

[See [Configuring a DHCP Client](#).]

IPv6

- **IPv6 packet (pps) and byte (bps) rates included in interface traffic statistics (MX series)**—Starting in Junos OS Release 18.1R1, the output of the following commands are modified:
 - The **show interfaces** command displays the input and output bytes (bps) and packets (pps) rates individually for IPv6 family in the IPv6 interface traffic statistics.
 - The **monitor interface** command displays the IPV6 interface traffic statistics along with input and output bytes (bps) and packets (pps) rates individually for IPv6 family.

[See [show interfaces](#) and [monitor interface](#).]

Junos OS XML, API and Scripting

- **Automation script library additions and upgrades (MX240, MX480, MX960, and vMX routers)**—Starting in Junos OS Release 18.1R1, devices running Junos OS that support Python automation scripts include new and upgraded Python modules. Python automation scripts can leverage new on-box Python modules, including `appdirs`, `asn1crypto`, `cffi`, `cryptography`, `idna`, `libffi`, `packaging`, `psutil`, `pyasn1`, `pyparser`, and `pyparsing`, as well as upgraded versions of existing modules. The `psutil` module is available only on devices running Junos OS with upgraded FreeBSD, and only a subset of functions is supported.

[See [Overview of Python Modules Available on Devices Running Junos OS](#).]

Management

- **Expanded support for chassis sensors for Junos Telemetry Interface (MX Series Transport Series Routers)**—Starting with Junos OS Release 18.1R1, Junos Telemetry Interface (JTI) provides new sensors that expand optics and power information.

To export telemetry data from Juniper equipment to an external collector requires both Junos Telemetry Interface (JTI) and gRPC to be configured.

Enhanced sensor information is also supported through operational mode commands **show chassis fpc detail**, **show chassis power detail**, and **show chassis pic fpc-slot id pic-slot id**.

Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module.

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

- **“ON CHANGE” sensor support through gRPC Network Management Interface (gNMI) for Junos Telemetry Interface (MX Series)**—Starting with Junos OS Release 18.1R1, ON_CHANGE streaming of

Address Resolution Protocol (ARP), Network Discovery Protocol (NDP), and IP sensor information associated with interfaces is supported on Junos Telemetry Interface (JTI).

Periodical streaming of OpenConfig operational states and counters has been supported since Junos OS Release 16.1, exporting telemetry data from Juniper equipment to an external collector. While useful in collecting all the needed information and creating a baseline “snapshot,” periodical streaming is less useful for time-critical missions. In such instances, you can configure ON_CHANGE streaming for an external collector to receive information only when operational states experience a change in state.

To support ON_CHANGE streaming, Google has developed a new specification called gRPC Network Management Interface (gNMI) for the modification and retrieval of configurations from a network element. Additionally, the gNMI specification can be used to generate and control telemetry streams from a network element to a data collection system. Using the new gNMI specification, one gRPC service definition can provide a single implementation on a network element for both configuration and telemetry as well as a single NMS element to interact with a device by means of telemetry and configuration RPCs.

Information about the RPCs supporting this feature can be found in the gNMI Proto file version 0.4.0 (the supported version) and the specification released by Google at:

- <https://github.com/openconfig/reference/blob/master/rpc/gnmi/gnmi-specification.md>
- <https://github.com/openconfig/gnmi/blob/master/proto/gnmi/gnmi.proto>

The telemetry RPC **subscribe** under gNMI service supports ON_CHANGE streaming. RPC **subscribe** allows a client to request the target to send it values of particular paths within the data tree. Values may be streamed (STREAM), sent one-off on a long-lived channel (POLL), or sent one-off as a retrieval (ONCE).

If a subscription is made for a top level container with a sample frequency of 0, leaves with ON_CHANGE support are streamed based on events. Other leaves will not be streamed.

NOTE: In order to permit a device to decide which nodes will be streamed as ON_CHANGE and which will SAMPLE, the collector should subscribe for TARGET_DEFINED with sample_interval.

Streaming telemetry data through gRPC requires you to download the OpenConfig for Junos OS module.

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

- **Junos Events Sensor for the Junos Telemetry Interface (JTI) (MX240, MX480, MX960, MX2010, MX2020 with MPC1, MPC2, MPC3, MPC4, MPC5, MPC6, MPC7, MPC8, or MPC9)**—Starting in Junos OS Release 18.1R1, the Junos events sensor is available for streaming system event data through JTI. Previously, only interval-based statistical sensors were available for use with JTI. With the Junos events sensor, system events that are available through system logging (syslog) can now be streamed to telemetry collection systems, allowing more data to be streamed and collected in one location. This helps to give a better picture of overall system health through one interface.

See [sensor \(Junos Telemetry Interface\)](#).

- **PIC services and IPSec sensors for Junos Telemetry Interface (MX Series)**—Starting with Junos OS Release 18.1R1, Junos Telemetry Interface (JTI) provides support for gRPC-based IKE and GPB UDP-based PIC sensors. These sensors provide visibility for IPSec services on different service complexes and nodes.

Exported data is defined using an IP address and a UDP port. When an export interval expires, the most recent statistics collected by the sensors are gathered, placed in the payload of a UDP packet, and forwarded to a collector. A timestamp indicating when counters are read is included with the exported data to allow collectors to collate data. The timestamp also can determine if and when an event happened, such as a PIC hardware restart or if counters were cleared by means of the CLI.

The resource paths are:

- `/junos/services/spu/ipsec-vpn`
- `/junos/ike-security-associations/ike-security-association/`

To export telemetry data from Juniper equipment to an external collector requires both Junos Telemetry Interface (JTI) and gRPC to be configured.

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

- **Fabric statistics support on Junos Telemetry Interface (JTI) (MX Series)**—Starting with Junos OS Release 18.1R1, fabric statistics limited to streaming over GBP over UDP are now supported for export by means of gRPC. Statistics are exported whether encoded as native or as a third-party data model.

Fabric statistic data is collected and exported by the following two types of fabric sensors:

- Per Packet Forwarding Engine pair fabric sensor
- Summary Flexible Pic Concentrator (FPC) fabric sensor

Streaming telemetry data through gRPC requires you to download the OpenConfig for Junos OS module.

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

- **ON_CHANGE support for Junos Telemetry Interface (JTI) (MX Series)**—Starting with Junos OS Release 18.1R1, OpenConfig support through gRPC Remote Procedure Calls (gRPC) and JTI is extended to support client streaming and bidirectional streaming of telemetry sensor information.

APIs have been implemented in Junos based on Protobuf specifications released by Google for OpenConfig. These APIs perform configuration, operational state retrieval, and telemetry on Junos routers using gRPC as the transport mechanism.

Starting in Junos OS 18.1R1, client streaming and bidirectional streaming are supported. With client streaming, the client sends a stream of requests to the server instead of a single request. The server typically sends back a single response containing status details and optional trailing metadata. With bidirectional streaming, both client and server send a stream of requests and responses. The client starts the operation by invoking the RPC and the server receives the client metadata, method name, and deadline. The server can choose to send back its initial metadata or wait for the client to start sending requests. The client and server can read and write in any order. The streams operate completely independently.

Junos devices can be managed through API (RPC) prototypes:

- **rpc Capabilities (CapabilityRequest)**

Returns (CapabilityResponse). Allows the client to retrieve the set of capabilities that is supported by the target.

- **rpc Get (GetRequest)**

Returns (GetResponse). Retrieves a snapshot of data from the target.

- **rpc Set (SetRequest)**

Returns (SetResponse). Allows the client to modify the state of data on the target.

- **rpc Subscribe (stream SubscribeRequest)**

Returns (stream SubscribeResponse). Allows a client to request the target to send it values for particular paths within the data tree. These values may be streamed (STREAM) or sent one-off on a long-lived channel (POLL), or sent as a one-off retrieval (ONCE). If a subscription is made for a top-level container with a sample frequency of 0, leaves with ON_CHANGE support are streamed based on events. Other leaves will not be streamed.

Juniper Extension Toolkit (JET) support provides insight to users regarding the status of clients connected to JSD. JET support for gRPC includes expanding the maximum number of clients that can connect to JSD from 8 to 30 (the default remains 5). To specify the maximum number of connections, include the **max-connections** statement at the **[edit system services extension-service request-response grpc]** hierarchy level.

To provide information regarding the status of clients connected to JSD, issue the enhanced **show extension-service client information** command and include the **clients** or **servers** options. The **clients** option displays request-response client information. The **servers** option displays request-response server information.

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

Multicast

- **Translation for MVPN Type 5 routes to MSDP SA (MX Series)**—Starting in Junos OS Release 18.1R1, Junos supports MVPN-Type-5 route to MSDP-SA conversion as defined in RFC [draft-ietf-bess-mvpn-sa-to-msdp-00.txt](#). Previously, Junos only supported translation in the other direction, MSDP SA to MVPN Type 5.

The ability to convert next-generation multicast virtual private network (MVPN) Type 5 routes to Multicast Source Discovery Protocol (MSDP) source active (SA) makes it possible to reduce the number of MSDP sessions running between VPN customer rendezvous points (C-RPs). For example, instead of having MSDP running among all C-RPs in a deployment, the C-RPs could instead run their MSDP sessions with a single PE router configured for multiple MSDP peers. The PE router, now acting as a C-RP device, would receive MVPN SA Type 5 routes from the RP-PE or source PE router, convert those routes to MSDP, and then advertise the MSDP routes to its MSDP peers.

MVPN Type 5 SA routes are added to MVPN table and include a new Extended Community (EC), with the IPv4 address of the RP where the MVPN SA was generated. The Type 5 routes source and EC are additionally added to the MSDP table. Stale routes, including the EC, are removed via MSDP once the MVPN type 5 SA route is gone from the MVPN table.

Enable MVPN to MSDP conversion at the `[edit routing-instance name protocols mvpn mvpn-mode spt-only convert-sa-to-msdp]` hierarchy level.

You can verify whether MVPN type 5 routes are being correctly converted to MSDP SA by running the `[show msdp source-active instance name]` command.

[See [MVPN Concepts and Protocols](#).]

MPLS

- **RSVP-TE pop-and-forward LSP tunnels (MX Series routers with MPCs and MICs)**—Pop-and-forward LSPs introduce the notion of pre-installed per traffic engineering link pop labels that are shared by RSVP-TE LSPs that traverse these links. A transit label-switching router (LSR) allocates a unique pop label per traffic engineering link with a forwarding action to pop the label and forward the packet over that traffic engineering link should the label appear at the top of the packet. Starting in Junos OS Release 18.1R1, you can configure pop-and-forward LSPs to significantly reduce the required forwarding plane state, enabling the pop-and-forward tunnels to couple the feature benefits of the RSVP-TE control plane with the simplicity of the shared MPLS forwarding plane.

All the existing RSVP-TE functionalities, such as bandwidth admission control, LSP priorities, preemption, auto-bandwidth, and MPLS fast reroute continue to work with pop-and-forward tunnels.

[See [RSVP-TE Pop-and-Forward LSP Tunnels Overview](#).]

- **Localization of next-hop-based dynamic tunnels**—(MX Series) Next-hop-based dynamic generic routing encapsulation (GRE) tunnels and MPLS-over-UDP tunnels distribute forwarding information to all line cards on a device. As a result, the origination and termination states of all tunnels are built on the Packet Forwarding Engines (PFEs) on every line card on the device, limiting the maximum number of tunnels supported on the device to the tunnel capacity of a single line card. Starting in Junos OS Release 18.1R1,

you can configure next-hop-based dynamic tunnel localization to create the forwarding information only on the PFE of a line card that is designated as the anchor PFE. The PFEs on the other line cards on the device have state forwarding information to steer the packets to the anchor PFE.

[See [Next-Hop-Based Dynamic Tunnel Localization Overview](#).]

- **Support for static segment routing label switched path (MX Series)**—Starting with Junos OS 18.1R1 release, a set of explicit segment routing paths are configured on the ingress router of a non-colored static segment routing label switched path (LSP) by configuring the **segment-list** statement at the **[edit protocols source-packet-routing]** hierarchy level. You can configure the segment routing LSP by configuring the **source-routing-path** statement at **[edit protocols source-packet-routing]** hierarchy level. The segment routing LSP has a destination address and one or more primary paths and optionally secondary paths that refer to the segment list. Each segment list consists of a sequence of hops. For non-colored static segment routing LSP, the first hop of the segment list specifies an immediate next hop IP address and the second to Nth hop specifies the segment identifies (SID) labels corresponding to the link or node which the path traverses. The route to the destination of the segment routing LSP is installed in inet.3 table. The adjacency segments, node segments, and prefix segments can be provisioned on transit routers by configuring static MPLS segment LSPs at the **[protocols mpls static-label-switched-path]** hierarchy level

[See [static segment routing lsp](#).]

Network Management and Monitoring

- **sFlow support on MX Series devices**—Starting in Junos OS Release 18.1R1, you can configure sFlow technology (as a sFlow agent) on a MX Series device, to continuously monitor traffic at wire speed on all interfaces simultaneously. The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology randomly samples network packets and sends the samples to a remote monitoring station, which presents quantifiably accurate network traffic visibility information after collecting data for a reasonably long period. These remote monitoring stations are called collectors.

[See the [Understanding How to Use sFlow Technology for Network Monitoring on a MX Series Router](#).]

- **Resource monitor support for PS and RLT interfaces (MX Series)**—Starting in Junos OS Release 18.1R1, PS and RLT interfaces support resource monitoring throttling. If a configured resource limit is exceeded for any member of a PS or RLT interface, the resource monitor prevents subscriber login and increments a denied counter. The denied counters can be verified with the **show system resource-monitor summary** command. In addition, the **show subscribers** command displays subscribers per PIC/PFE/Slot for PS and RLT interfaces.

[See [resource-monitor](#).]

- **The bbe-mibd component is enhanced with additional MIB objects (MX Series)**—In the next-generation broadband edge architecture, subscribers are represented by flows instead of logical interfaces. The SNMP subagent bbe-mibd was implemented to handle SNMP requests for subscriber interfaces. As of Junos OS Release 18.1R1, the following MIB objects are made available for flow-based dynamic interfaces as part of bbe-mibd:

- ifChassisTable
- ipv6IfTable
- ipv6IfStatsTable
- jnxIpv6

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

- **Enhancement to Junos OS SNMP MIB PCC functionality (MX Series)**—Starting in Junos OS Release 18.1R1, Junos OS provides enhanced MIB support for Path Computation Clients. This enhancement enables the Path Computation Client (PCC) process to accept SNMP **get** and **getnext** commands for Path Computation Client Protocol (PCEP) peer and PCEP session tables and reply to them. This feature monitors PCEP interactions between a PCC and a Path Computation Element (PCE). Not all members of PCEP peer and PCEP session tables mentioned in the RFC (RFC 7420) are supported. For exceptions, see [Standard SNMP MIBs Supported by Junos OS](#).

[See [MIB Explorer](#). Name of MIB is **pcep.mib**.]

Operation, Administration, and Maintenance (OAM)

- **CFM Action Profile to Bring Down a Group of Logical Interfaces(MX Series Routers)**—Starting with Junos OS Release 18.1R1, you can create a CFM Action Profile and define an action to bring down a group of logical interfaces using CFM session configured on a single IFL. Following new configuration statements are introduced:
 - To mark the interface group down configure **interface-group-down** at the **[edit protocols oam ethernet connectivity-fault-management action-profile *action-profile-name*** hierarchy level.
 - To mark the interface group down for the action profile configured with the action **interface-group-down**, configure **interface-group(*interface-device-name* | *unit-list*)** at the **[edit protocols ethernet connectivity-fault-management maintenance-domain *md-name* maintenance-association *ma-name* mep *mep-id* remote-mep *mep-id* action-profile *profile-name*** hierarchy level. The ***interface-device-name*** represents an Ethernet interface device. The ***unit-list*** defines a string of logical unit numbers.

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

Routing Policy and Firewall Filters

- **Firewall filters and policers for abstracted fabric interface (MX Series)**—Starting with Junos OS Release 18.1R1, you can configure firewall filters and policers on an abstracted fabric (AF) interface, a pseudointerface that facilitates routing control and management traffic between guest network functions (GNFs) through the switch fabric. AF interfaces support single-rate two-color policer, single-rate three-color policer, two-rate three-color policer, and hierarchical policer. The AF interface firewall filters are supported on Inet, Inet6, MPLS, and CCC protocol families.

NOTE: The AF interface bandwidth is assigned to all FPCs linked to that AF interface. Therefore, a policer bandwidth limit configuration on an AF interface is applicable to all the PFEs associated with the AF interface.

[See [Understanding the Use of Policers in Firewall Filters](#).]

Routing Protocols

- **Support for BGP multipath at global level (MX Series)**—Starting with Junos OS Release 18.1R1, BGP multipath is available at the global level in addition to the group and neighbor level. In earlier Junos OS releases BGP multipath is supported only at the group and neighbor levels. A new configuration option **disable** is available at the **[edit protocols bgp multipath]** hierarchy level to disable BGP multipath for specific groups or neighbors. This allows you to configure BGP multipath globally and disable it for specific groups according to your network requirements.

[See [disable](#).]

- **Support for BGP Labeled Unicast traffic statistics collection (MX Series)** —Starting in Junos OS Release 18.1R1, you can enable traffic statistics collection for BGP labeled unicast traffic at the ingress router. In a network configured with segment routing, traffic statistics can be collected periodically based on the label stack received in the BGP route update and saved in a specified file. Traffic statistics collection is supported only for IPv4 and IPv6 address families.

[See [Enabling Traffic Statistics Collection for BGP Labeled Unicast](#).]

- **Multipath optimization to improve RIB learning rate**—Starting in Junos OS Release 18.1R1, you can defer multipath calculation until all BGP routes are received. When multipath is enabled, BGP inserts the route into the multipath queue each time a new route is added or whenever an existing route changes. When multiple paths are received through BGP add-path feature, BGP might calculate one multipath route multiple times. Multipath calculation slows down the RIB (also known as the routing table) learning rate. To speed up RIB learning, multipath calculation can be either deferred until the BGP routes are received or you can lower the priority of the multipath build job as per your requirements until the BGP routes are resolved.

To defer the multipath calculation configure **defer-initial-multipath-build** at **[edit protocols bgp]** hierarchy level. Alternatively, you can lower the BGP multipath build job priority using **multipath-build-priority** configuration statement at **[edit protocols bgp]** hierarchy level to speed up RIB learning.

[See [defer-initial-multipath-build](#).]

Security

- **Secure Boot (MX240, MX480, MX960, MX2010, and MX2020 that use Routing Engines RE-S-X6-128G or RE-MX2K-X8-128G)**—Starting in Junos OS Release 18.1R1, 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 and thus safeguarded from tampering or modification. Secure boot is enabled by default on supported platforms.

[See [Feature Explorer](#) and enter **Secure Boot**.]

Services Applications

- **Support for additional DS-Lite features on MS-MPCs and MS-MICs (MX Series routers)**—Starting in Junos OS Release 18.1R1, dual-stack lite (DS-Lite) running on MS-MPCs and MS-MICs adds support for the following features:
 - ALGs (TFTP, FTP, DNS, ICMP, RTSP, PPTP)
 - Configurable MTU per software concentrator
 - IPv6 fragmentation and reassembly
 - NAPT-44 port block allocation
 - Receiving and transmitting IPv4 fragments in IPv6
 - Traceroute through the software tunnel
 - Hairpinning with NAPT-44 EIF

Prior to Junos OS Release 18.1R1, DS-Lite did not support these feature on the MS-MPCs and MS-MICs.

[See [Tunneling Services for IPv4-to-IPv6 Transition Overview](#).]

- **Support for IPv6 version 9 templates for inline active flow monitoring (MX Series)**—Starting in Junos OS Release 18.1R1, you can apply version 9 flow templates to IPv6 traffic when using inline flow monitoring. In addition, fields have been added to several IPFIX and version 9 templates for inline flow monitoring to make the templates more uniform for each supported family.

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

- **Support for additional filtering on show command output of RPM probes generated on an MS-MPC or MS-MIC (MX Series)**—Starting in Junos OS Release 18.1R1, you can use new filters to limit the output of the **show services rpm probe-results** and **show services rpm history-results** commands for real-time processing (RPM) probes that are generated on an MS-MPC or MS-MIC.

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

- **Support for generating IPv6 RPM probes on MS-MPCs and MS-MICs (MX Series)**—Starting in Junos OS Release 18.1R1, you can configure an MS-MPC or MS-MIC to generate **icmp6-ping** real-time performance monitoring (RPM) probes. Generating RPM probes on an MS-MPC or MS-MIC increases the number of probes that can run at the same time, compared to probes that are generated on the Packet Forwarding Engine.

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

Software Defined Networking

- **MS-MIC and MS-MPC support for Junos Node Slicing (MX480, MX960, MX2010, MX2020)**—Starting from Junos OS Release 18.1R1, Junos Node Slicing supports assignment of MS-MICs and MS-MPCs to guest network functions (GNFs). MS-MICs and MS-MPCs provide improved scaling and high performance, and possess enhanced memory (16 GB for MS-MIC; 32 GB per NPU of MS-MPC) and processing capabilities. The MS-MIC supports the Layer 3 services such as stateful firewall, NAT, IPsec, active flow monitoring, RPM, and graceful Routing Engine switchover (GRES).

[See [Multiservices MIC and Multiservices MPC \(MS-MIC and MS-MPC\) Overview](#).]

Subscriber Management and Services

- **Controlling search behavior for address allocation from linked pools (MX Series)**—Starting in Junos OS Release 18.1R1, you can use the **linked-pool-aggregation** statement at the **[edit access address-assignment pool pool-name]** 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](#).]

- **Support for Packet triggered subscriber functionality (MX Series)**—Starting with Junos OS 18.1R1, support for packet triggered subscriber functionality creates IP demux IFL on receiving a data packet from clients with pre-assigned IP address using a new demux configuration at the hierarchy level **[edit interfaces interface-name unit unit-number]**.

[See [IP demultiplexing interfaces on Packet-Triggered Subscribers Services Overview](#).]

- **BPCEF Gy Assume Positive CCR-T File Support (MX Series)**—Starting with Junos OS 18.1R1, broadband PCEF provides the file backup for OCS data when both primary and alternative paths to the OCS are not available. The CCR-GY-T frames are stored in the files on remote location. The backup is supported at the hierarchy **[edit access ocs partition partition-name]**.

[See [Gy File Backup Overview](#).]

- **Support for per-subscriber MTU for dynamic profiles of IP v4 or IPv6 protocol family (MX Series)**—Starting with Junos OS 18.1R1, maximum transmission unit (MTU) can be configured per subscriber for dynamic profiles. The value of MTU can be static or represented through

\$junos-interface-mtu variable. By default, the variable value is the MTU of the payload that is less than the MTU of the physical interface minus the family protocol overhead. A specific value is returned through RADIUS authentication through the framed MTU attribute. If the RADIUS fails to return framed MTU value for \$junos-interface-mtu variable then the default value from **interface-mtu** statement at **[edit dynamic-profiles profile-name predefined-variable-defaults]** hierarchy level. You can configure value for **mtu** statement at **[edit dynamic-profiles name interfaces name unit name family inet]** hierarchy level or at **[edit dynamic-profiles name interfaces name unit name family inet6]** hierarchy level.

[See [Per-subscriber support of maximum transmission unit for dynamic profiles.](#)]

- **Enhancements to dual-stack, single-session authentication and reauthentication (MX Series)**—Starting in Junos OS Release 18.1R1, reauthentication is supported in response to DHCP discover and solicit messages, in addition to the previously supported renew and rebind messages.

Reauthentication is supported for DHCP dual-stack, single-session subscribers when on-demand address allocation is configured. Both authentication and reauthentication for dual-stack, single-session supports are performed per family in the stack, using separate Access-Requests to the RADIUS server.

[See [RADIUS Reauthentication As an Alternative to RADIUS CoA for DHCP Subscribers.](#)]

- **Excluding addresses or ranges to manage address allocation pools for DHCP local server (MX Series)**—Starting in Junos OS Release 18.1R1, you can exclude IPv4 or IPv6 individual addresses or ranges of consecutive addresses within an address pool from being allocated to subscribers. If you exclude an address that has already been allocated, the subscriber is logged out, the address is deallocated, and then marked for exclusion.

[See [Preventing Addresses from Being Allocated from an Address Pool.](#)]

- **Preventing validation of magic numbers in PPP peer-originated keepalive messages (MX Series)**—Starting in Junos OS Release 18.1R1, you can include the **ignore-magic-number-mismatch** statement to disable the Packet Forwarding Engine from validating PPP magic numbers received during PPP keepalive (Echo-Request/Echo-Reply) exchanges. Because validation is not performed, the Packet Forwarding Engine does not detect whether the remote peer sends a magic number that does not match the number agreed upon during LCP negotiation. This prevents PPP from tearing down the session in the event of a mismatch. This capability is useful when the remote PPP peers include arbitrary magic numbers in the keepalive packets. Configuring this statement has no effect on LCP magic number negotiation or on the exchange of keepalives when the remote peer magic number is the expected negotiated number.

[See [Preventing the Validation of PPP Magic Number During PPP Keepalive Exchanges](#) and [Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile.](#)]

- **Local dynamic service profile activation on L2TP login (MX Series)**—Starting in Junos OS Release 18.1R1, you can use dynamic service profiles to apply services to all subscribers in a tunnel group or to all subscribers using a particular LAC without involving RADIUS. In multivendor environments, customers might use only standard RADIUS attributes to simplify management by avoiding the use of vendor-specific attributes (VSAs) from multiple vendors. However, VSAs are generally required to apply services. Local service profile activation enables you to avoid that problem. It can also be a way to provide default

services when RADIUS servers are down. You can also pass parameters to the services as they are applied, such as a downstream shaping rate for a CoS service.

[See [Applying Services to an L2TP Session Without Using RADIUS.](#)]

- **Changes to JSRC Provisioning for Dual-Stack Subscribers (MX Series)**—Starting in Junos OS Release 18.1R1, you can include the **dualstack-support** statement at the **[edit jsrc]** hierarchy level to configure JSRC provisioning for dual-stack subscribers so that JSRC reports information about the separate stacks for a given subscriber, using a single JSRC session. Accounting statistics are reported separately for each family. In earlier releases, the remote SRC peer is not informed about whether only on family or both families are active, and all statistics are aggregated across the families.

[See [JSRC Provisioning for Dual-Stack Subscribers.](#)]

- **Providing L2TP service rate limits at subscriber login (MX Series)**—Starting in Junos OS Release 18.1R1, you can specify the name of the dynamic service profile that provides values for the transmit (Tx) and receive (Rx) connect speeds for traffic between the LAC and the subscriber. When that profile name is returned in the Juniper Networks Activate-Service VSA (26-65) in the RADIUS Access-Accept message at subscriber login, the values are converted from Kbps to bps and stored in the session database. You can also modify the rates with parameters passed in the VSA or specify an adjustment for the values, up or down, in the CLI. The rates are sent in the ICCN message from the LAC to the LNS as AVP 24 and AVP 38.

[See [Specifying a Rate-Limiting Service Profile for L2TP Connection Speeds.](#)]

- **Flexible filtering of RADIUS attributes and VSAs (MX Series)**—Starting in Junos OS Release 18.1R1, a flexible configuration method is supported for filtering undesirable RADIUS standard attributes and vendor-specific attributes (VSAs). Attributes received from RADIUS take precedence over internally provisioned attributes; filtering ensures that the corresponding internally provisioned attribute values are used.

The flexible configuration enables you to specify RADIUS standard attributes with the attribute number, and to specify VSAs with the IANA-assigned vendor ID and the VSA number. Some attributes can be ignored when received in Access-Accept messages; other attributes can be excluded from Access-Request and accounting messages. Only those standard attributes and VSAs supported by your platform can be filtered. You can configure unsupported standard attributes, vendors, and VSAs, but the configuration has no effect.

In earlier releases, you must specify dedicated keywords (options) for attributes to filter. This method is still supported. If you configure filtering with both methods, attributes that are specified with either method are filtered.

[See [Enabling the Use of Local Values by Filtering RADIUS Attributes and VSAs.](#)]

- **Additional RADIUS attributes and VSAs supported for filtering (MX Series)**—Starting in Junos OS Release 18.1R1, you can filter the following attributes from RADIUS Access-Accept messages with the **ignore** statement:

Standard RADIUS attributes:

- Session-Timeout (27)
- Idle-Timeout (28)

Microsoft (IANA vendor-id 311) vendor specific attributes:

- MS-Primary-DNS-Server (26-28)
- MS-Secondary-DNS-Server (26-29)

[See [ignore](#).]

User Interface and Configuration

- **Ephemeral configuration database support for load replace and load override operations (MX Series)**—Starting in Junos OS Release 18.1R1, NETCONF and Junos XML protocol client applications can configure the ephemeral configuration database using **load replace** and **load override** operations, in addition to the previously supported **load merge** and **load set** operations. To perform a **load replace** or **load override** operation, set the **<load-configuration> action** attribute to **replace** or **override**, respectively.

[See [Configuring Ephemeral Database Instances](#).]

VPNs

- **Support for seamless migration from BGP-VPLS to EVPN (MX Series)**—Starting in Junos OS Release 18.1R1, a solution is introduced for enabling staged migration from BGP-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 co-exist. The solution supports single-active redundancy of multi-homed networks and multi-homed devices for EVPN PEs. With single-active redundancy, the participant VPN instances may span across both EVPN PEs and VPLS PEs as long as single-active redundancy is employed by EVPN PEs.

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

SEE ALSO

[Changes in Behavior and Syntax | 110](#)

[Known Behavior | 115](#)

[Known Issues | 119](#)

[Resolved Issues | 128](#)

[Documentation Updates | 154](#)

[Migration, Upgrade, and Downgrade Instructions | 155](#)

[Product Compatibility | 162](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [EVPNs | 110](#)
- [High Availability \(HA\) and Resiliency | 111](#)
- [Interfaces and Chassis | 111](#)
- [Management | 112](#)
- [MPLS | 112](#)
- [Network Management and Monitoring | 112](#)
- [Network Operations and Troubleshooting Automation | 113](#)
- [Routing Protocols | 113](#)
- [Software Defined Networking | 113](#)
- [Subscriber Management and Services | 114](#)
- [User Interface and Configuration | 115](#)

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 18.1R2 for MX Series routers.

EVPNs

- **Change in the output for `show evpn instance` and `show evpn database`**—Starting in Junos OS Release 18.1R1, the output for `show evpn instance` and `show evpn database` displays a local interface with an interface name of `.local..number`, and no configuration. This interface is created to support configuration fault management (CFM). For example, `show evpn instance` displays the following sample output.

```
Number of local interfaces: 2 (2 up)
  Interface name  ESI                                     Mode          Status
  AC-Role
    .local..9      00:00:00:00:00:00:00:00:00:00  single-homed  Up
  Root
```

- **Support for LSP on EVPN-MPLS**—Starting in Junos OS Release 18.1R1, Junos OS 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 18.1R1, 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>

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)**.

Interfaces and Chassis

- **Modified output of the request vmhost zeroize command**—The command **request vmhost zeroize**, upon execution, prompts the user for confirmation to proceed. The following line is displayed:

```
user@host request vmhost zeroize
VMHost Zeroization : Erase all data, including configuration and log files ?
[yes,no] (no) yes
```

See [request vmhost zeroize](#).

- **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 18.1R1, 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.

[See [flow-control-options](#)]

Management

- **Enhancement to LSP statistics sensor for Junos Telemetry Interface (MX Series)**—Starting with Junos OS Release 18.1R1, the telemetry data exported for the LSP statistics sensor no longer includes the phrase **and source 0.0.0.0** after the LSP name in the value string for the prefix key. This change reduces the payload size of data exported. The following is an example of the new format:

```
str_value: /mpls/lsp/constrained-path/tunnels/tunnel[name='LSP-4-3']/state/
counters[name='c-27810']/
```

- **Enhancement to NPU memory sensors for Junos Telemetry Interface (MX Series)**—Starting with Junos OS Release 18.1R1, the format of telemetry data exported through gRPC for NPU memory and memory utilization implements prefix compression. This change reduces the payload size of data exported. The following example shows the new format:

```
key: __prefix__
```

```
str_value: /components/component[name='FPC0:NPU0']/properties/property
```

```
key: [name='mem-util-edmem-size']/value
```

```
uint_value: 12345
```

Telemetry data is exported in key-value pairs. Previously, the data exported included the component and property names in a single key string.

MPLS

- **Support for inet.0 and inet.3 labeled unicast BGP route for protocol LDP (MX Series)**--- Starting in Junos OS Release **18.1R2**, 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 OS Release 16.1R1, LDP egress policy was supported in inet.3 RIBs, in addition to inet.0 RIBs, for labeled-unicast BGP routes.
- Starting in Junos OS Release 18.1, a new option – **name lsp-name** – is introduced in the **show mpls lsp autobandwidth** command to specify the name of the LSP for which the autobandwidth information is displayed. With the **name** option, the autobandwidth information specific to the LSP name that has been provided can be obtained in the command output.

[See [show mpls lsp autobandwidth](#).]

Network Management and Monitoring

- **SNMP syslog messages changed (MX Series)**—In Junos OS Release 18.1R1, 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](#).]

- **Customer-visible SNMP trap name changes (MX Series)**—In Junos OS Release 18.1R1, on the source control board enhanced (SCBE), name changes include the CB 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 SNMP trap interface name (jnxClkSyncIntfName), for example, value: "external(cb-0)".

See [SNMP MIB Explorer](#).

Network Operations and Troubleshooting Automation

- **JET - Correction to escaped characters notification events (MX Series and vMX routers)**—Per RFC7159, certain characters must be escaped. Data returned from JET notification subscriptions contained escaped characters that were not required. This has been corrected to comply with RFC7159.
- **respawn-on-normal-exit** option added to [edit system extensions extension-service application file <application-name>] hierarchy (MX Series routers and vMX)—This option helps to ensure that daemonized Juniper Extension Toolkit (JET) applications that exit normally will restart without user intervention. Daemonized JET applications that exit unexpectedly will still restart without user intervention. This is the default behavior.

Routing Protocols

- **show isis database command output enhanced**— Starting in Junos OS Release 18.1R1, the output of **show isis database** command includes the *Extended IS Reachability* TLV type and length fields. The output also includes the SubTLV length of IS extended neighbors, which helps in understanding the order in which the IS-IS neighbors are packed in the *Extended IS Reachability* TLV.

[See [show isis database](#).]

Software Defined Networking

- **Revoking delegation of PCE-initiated LSPs**—Starting in Junos OS Release 18.1, for a PCC to revoke the delegation of PCE-initiated LSPs, the **lsp-cleanup-timer** must be greater than or equal to the **delegation-cleanup-timeout** at the [edit protocol pcep pce pce-name] hierarchy level. If not, the redelegation timeout interval for the PCC can be set to infinity, where the LSP delegations to that PCE remain intact until specific action is taken by the PCC to change the parameters set by the PCE.

- **The 32-bit libstdc++6 package no longer required for Junos Node Slicing setup**—Starting in Junos OS Release 18.1R2, you need not install the additional 32-bit `libstdc++` package for Red Hat Enterprise Linux (RHEL) or Ubuntu to set up Junos Node Slicing.

Subscriber Management and Services

- **Change to ICRQ message inclusion of the ANCP Access Line Type AVP (MX Series)**—Starting in Junos OS Release 18.1R1, 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.

[See [Subscriber Access Line Information Handling by the LAC and LNS Overview](#).]

- **Support for IPv6 all-routers address in nondefault routing instance (MX Series)**—Starting in Junos OS Release 18.1R1, 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 18.1R1, 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 18.1R2, 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.

- **Changes in recommendations for maximum configuration database size (MX Series)**—Starting in Junos OS Release 18.1R2, we recommend that you allow the router to determine the appropriate size for the configuration database to optimize the amount of shared memory available for subscriber management. Do not configure a maximum size.

This recommendation applies to MX240, MX480, MX960, MX2008, MX2010, MX2020, and MX10003 routers when all the Routing Engines have at least 32GB of RAM each. When the Routing Engines have less RAM, we recommend that you configure the maximum size to no more than 300MB.

[See [Configuring Junos OS Enhanced Subscriber Management](#).]

User Interface and Configuration

- Junos OS prohibits configuring ephemeral configuration database instances that use the name **default** (MX Series)—Starting in Junos OS Release 18.1R1, user-defined instances of the ephemeral configuration database, 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**.

SEE ALSO

[New and Changed Features | 90](#)

[Known Behavior | 115](#)

[Known Issues | 119](#)

[Resolved Issues | 128](#)

[Documentation Updates | 154](#)

[Migration, Upgrade, and Downgrade Instructions | 155](#)

[Product Compatibility | 162](#)

Known Behavior

IN THIS SECTION

- [EVPN | 116](#)
- [General Routing | 116](#)
- [Interfaces and Chassis | 117](#)
- [MPLS | 118](#)
- [Platform and Infrastructure | 118](#)
- [Routing Protocols | 118](#)
- [Services Applications | 118](#)
- [Software Installation and Upgrade | 118](#)

This section contains the known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.1R2 for MX Series routers.

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

EVPN

- When the Routing Engine switchover in a scaled-up EVPN VPWS configurations (approximately 8000 EVPN VPWS), the rpd scheduler slip messages might be seen. [PR1225153](#)

General Routing

- 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 configuring the XE interface. The netdev interface resource determines that speed is a configurable parameter that is supported on a GE interface but not on an XE interface. Hence, the 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](#)
- On rebooting, RHEL 7.3 servers report libvirtd[6282]: segfault at 10 ip 00007f87eab09bd0. No core file is left and no operational impact is known. [PR1287808](#)
- For CFP2-DCO-T-WDM-1 pluggable, Rx payload type shown incorrectly (shown 0 vs 7). [PR1300423](#)
- IPsec operations are optimized for smaller packet size (up to ~1900 bytes) on MS-MPC and MS-MIC platforms thus yielding higher throughput and lower latency for more common network deployments. A slightly higher latency might be seen if there are jumbo packets in the network. [PR1307867](#)
- Sometimes 1GE interface might remain down after certain events. The events that might cause 1GE interface to remain down are as follows:
 - The two interfaces are connected in loopback on 12 Port QSFP28 TIC on MX10003 or 4 Port QSPF28 fixed PIC on MX204 and configured as 1GE interfaces.
 - When two MX10003 boxes and configured in 1G are connected back to back and rebooted at same time with 1GE interfaces on 12 Port QSFP28 TIC. [PR1312403](#)
- With 1GE interfaces configured on either MX10003 or MX204, the available throughput per port will be in the order of approximately 990mbps instead of 1000mbps (1Gbps) [PR1318293](#)
- Starting in Junos OS Release 15.1, the enhanced subscriber management SNMP interface filters might not work for subscriber interfaces when "interface-mib" is part of subscriber dynamic-profile. Without "interface-mib" in subscriber dynamic profile, there is no change in behavior. [PR1324573](#)

- In MX Series routers, when Telemetry is enabled upon GRES, IKE sensor subscription from collector should restart new backup Routing Engine that still holds the old subscription state, which is functionally dormant, until it becomes an active Routing Engine again. When it becomes a master Routing Engine, no stale state is held. New IKE sensors are added with new subscription from remote collectors. [PR1340110](#)
- When a new instance of Virtual Route Reflector (VRR) is launched, the factory default configuration has DHCP client and auto image is turned on. Even after DHCP configuration is removed, access-internal default routes installed by DHCP client might persist and cause reachability problem. This typically happens during initial installation, and restart routing immediately might clear the problem. [PR1335925](#)

Interfaces and Chassis

- In case of hw-assisted-pm mode of operation at responder, it takes few ms/seconds (based on the programmed scale) to program inline-responder entries once CCM comes up, So till inline-entry corresponding to a SLM session doesn't get programmed response will not be send back to originator and originator will see loss. Once inline-responder entry gets programmed responses will be sent back to originator. [PR1311963](#)
- For MIC-3D-8OC3-2OC12-ATM on MX104 routers, ensure that the configured **cell-bundle-size** is less than 30 for an ATM interface that is configured with **atm-ccc-cell-relay** encapsulation. If the configured **cell-bundle-size** is greater than or equal to 30 and the traffic is passing through the interface at line rate, it might lead to AFEB crash.

[See [cell-bundle-size](#)]

- At JDM install time, each JDM instance generates pseudo random MAC addresses to be used for JDM's own management interface and for the associated GNFs' management interfaces. At GNF creation time, each GNF instance generates pseudo random MAC addresses to be used as the chassis MAC address pool for the forwarding interfaces of that GNF. Once generated, JDM and GNF MAC addresses are persistent, and will only be deleted when the JDM or GNF instance itself is deleted.

At a GNF, the Junos OS CLI command **show chassis mac-addresses** can be used to examine its chassis MAC address pool, and the Junos OS CLI command **show interfaces fxp0** can be used to examine the MAC address of its management interface.

At JDM, the CLI command **show interfaces jmgmt0** can be used to examine the MAC address of its management interface.

In case of MAC address duplication across JDM or GNF instances, you must delete and then reinstall the respective JDM or GNF instance and check again for duplication.

MPLS

- An SR-TE path with "0" explicit NULL as inner most label, SR-TE path does not get installed with label "0". [PR1287354](#)

Platform and Infrastructure

- The Junos OS does not launch `/usr/sbin/commitd -s` after every switchover. [PR1284271](#)

Routing Protocols

- When an Junos OS aggregation gateway uses a IPv6 address as a next hop for IPv4 aggregates announced to downstream, it might attract the 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](#)
- BGP peer flap is seen when Routing Engine switchover is triggered from old backup Routing Engine. This issue is seen only with higher scales. The issue is related to slow draining out of new backup socket. [PR1325804](#)

Services Applications

- It is not recommended to configure **ms- interface** when AMS bundle in one-to-one mode has the same member interface. [PR1209660](#)

Software Installation and Upgrade

- **Unified ISSU with active BBE subscribers using advanced services supported only to 18.1R2 and later 18.1 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 18.1 release earlier than 18.1R2. If you perform an ISSU to an 18.1 release earlier than 18.1R2, the advanced services PCC rules are not attached to subscribers.

SEE ALSO

[New and Changed Features | 90](#)

[Changes in Behavior and Syntax | 110](#)

[Known Issues | 119](#)

[Resolved Issues | 128](#)

[Documentation Updates | 154](#)

[Migration, Upgrade, and Downgrade Instructions | 155](#)

[Product Compatibility | 162](#)

Known Issues

IN THIS SECTION

- [EVPN | 120](#)
- [Forwarding and Sampling | 121](#)
- [General Routing | 121](#)
- [Infrastructure | 123](#)
- [Interfaces and Chassis | 124](#)
- [Layer 2 Features | 124](#)
- [MPLS | 125](#)
- [Platform and Infrastructure | 125](#)
- [Routing Protocols | 126](#)
- [Services Applications | 127](#)
- [Subscriber Access Management | 127](#)
- [VPNs | 128](#)

This section lists the known issues in hardware and software in Junos OS Release 18.1R2 for MX Series routers.

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

EVPN

- L2-learning process (l2ald) might generate a core file in a scaled Layer 2 setup, including bridge domain, VPLS, EVPN, and so on. The l2ald process follows a kernel page. In most cases, the issue is recovered on its own after the l2ald core file is generated. In some cases, a manual restart of the process is required 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. Core dumped! . [PR1142719](#)**
- When you run VPLS on MX Series routers (with Junos OS), you might have statements such as **mac-table-size** configured under the **[routing-instance protocols vpls]** hierarchy. You can also configure these statements under **[protocols evpn]** for an EVPN routing instance. When you migrate a VPLS instance to EVPN, you do not need to configure the attributes under **[protocols evpn]**; which means that the configuration under **[protocols evpn]** continue to be in effect. But when the VPLS protocol is eventually disabled (so that it does not interfere with EVPN after all nodes are migrated), you must configure the statements under **[protocols evpn]**. Otherwise, the configuration reverts to default values for the routing instance and results in the removal of all dynamically learned MAC addresses, which is also known as MAC flush processing. [PR1312531](#)
- If a host is multihomed to a set of PE devices for redundancy, when the host's MAC or IP address is learned by one of these PE devices, then all PE devices belonging to this redundant set will 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 configuration statement **routing-option forwarding-table chained-composite-next-hop ingress evpn** on a QFX5110 platform unless this configuration statement is a part of the Junos OS default configuration. Otherwise, without enabling this configuration statement, if a PE device is attached to the multihomed end system (ES) learned this host's MAC or IP address only from the control plane through EVPN, the PE device installs the /32 host route pointing to the remote PE device where it learned host's MAC or IP address. For a PE device attached to the multihomed end system (ES) and learned by this host's MAC or IP address locally through the data plane, the PE device always installs the /32 host route pointed to its local IRB interface. [PR1321187](#)
- When there is a direct connection between leaf to leaf, there might be a scenario where MAC is learned on a VTEP tunnel from a remote switching gateway instead of on a local interface. The MAC in question is behind the CE connected to both leaves in active-active mode. There is a temporary loop during the system bring up. [PR1323182](#)
- Provider backbone bridging (PBB) EVPN is unable to flood traffic toward the core. To recover traffic, use the **restart l2-learning** command. In addition to this, there is a limitation in PBB EVPN active/active unicast traffic forwarding. If entropy in the traffic is not sufficient, then uneven load balancing causes a problem on MH peer active/active routers. The two problems mentioned here are applicable to MAC-in-MAC PBB-EVPN and does not affect any other scenario. [PR1323503](#)
- In Junos OS platform, the l2ald daemon might crash when MAC address processing. The MAC learning process will be impacted during the period of l2ald crash. The l2ald recovers itself. [PR1347606](#)

Forwarding and Sampling

- When a policing filter is applied to an active LSP carrying traffic, the LSP re-signals 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 a policing filter and a policing filter application to the LSP through 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](#)

General Routing

- SIP session fails when an IPv4 SIP client in a public network initiates a SIP call with an IPv6 SIP client in the private network. [PR1139008](#)
- If the PIC type (4x OC-12-3 SFP) is replaced with the PIC type (4 x OC-3 1x OC-12 SFP) on the device and the configuration is committed, the PIC type (4 x OC-3 1x OC-12 SFP) might bounce. This bounce is noticed with the first commit after the replacement. [PR1190569](#)
- Malicious LLDP crafted packet leads to privilege escalation, denial of service (CVE-2018-0007). Refer to <https://kb.juniper.net/JSA10830> for more information. [PR1252823](#)
- When an interface comes online and both the OAM protocol and the MKA protocol try to establish their respective sessions, OAM takes the interface down and MKA fails to establish connection (because the interface is down, it cannot send out MKA packets). [PR1265352](#)
- On MPC2E-NG, MPC3E-NG, MPC5E, MPC6E, MPC7E, MPC8E, and MPC9E line cards, a firewall performance feature fast-lookup-filter can be activated. Because of the transient parity error, the packet is dropped within the PPE with the **sync xtxn error** message. This issue might adversely impact traffic, which might eventually affect the service. [PR1266879](#)
- Dynamic endpoint (DEP) does not support the dh group group19, the encryption algorithm aes-256-cbc, and the hash sha-384 in its list of default proposals. These must be configured explicitly in the configuration. [PR1269160](#)
- In an inline J-Flow, when the **template-refresh-rate** and **option-refresh-rate** CLI statements are configured with both **packets interval** and **seconds interval** configuration options, the **packets interval** configuration does not work. [PR1274206](#)
- The MPC7E, MPC8E, and MPC9E line cards might not come up online after installing or rebooting the MPC. [PR1279344](#)
- If VM host snapshot is taken on an alternate disk and there is no further VM host software image upgrade, the expectation is that the currently corrupt VM host image can use the alternate disk to recover the primary disk state. However, if the host file system is corrupted, the node boots from the previous VM host software instead of booting from the alternate disk. [PR1281554](#)
- Because of the vendor code limitation, ungraceful removing of summit MACsec TIC from the chassis might crash or give unpredictable results. [PR1284040](#)

- The Routing Engine get stuck and boots from the other SSD after vmhost reboot. You must boot the Routing Engine from the primary SSD. [PR1295219](#)
- In some Junos OS MX Series router deployments, random syslog messages are observed for FPC cards. **fpcx ppe_img_ucose_redistribute Failed to evict needed instr to GUMEM - xxx left**. These messages are not an issue and might not cause any 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](#)
- When a GRES or NSR is performed on a base system (BSYS), the master Routing Engine on the guest network functions (virtual nodes or network slices) detects the BSYS chassisd restart and enters an NSR hold down delay. During this time, CLI commands evoke a switchover on the master Routing Engine indicating that the system is not NSR ready. This situation is similar to that of a standalone MX Series router in which chassisd is restarted on the master Routing Engine. Note that the CLI command on the BU Routing Engine will succeed. This too is similar to standalone MX Series router behavior. [PR1298571](#)
- Internal latency is high during initial subscription of sensors when multiple sensors (in order of 15-20) are subscribed together. This is not observed with a lesser number of subscriptions. This is for a small period when sensors are being installed. [PR1303393](#)
- The mgd process might crash and generate a core file.
@thr_kill,ppool_bkt,ppool_get_offset,ppool_fetch,dbm_offset_fetch. [PR1305424](#)
- If syslog errors **pfeman_inline_ka_steering_gencfg_handler: nh not found for nh=<pfh nhid** are seen on the FPC after it reboots, it is likely that steering rules used for BFD packet redirection are not installed correctly. This might be caused because of an unexpected replay order of IPC messages from the kernel when the FPC reboots. It might be advisable to reconfigure the impacted BFD sessions that use the respective <pf nhid> for the redirect rules. [PR1308884](#)
- Support for enterprise profile is provided only for 10 Gigabit Ethernet interfaces. Use of 40 Gigabit Ethernet and 100 Gigabit Ethernet interfaces might result in a phase alignment issue. [PR1310048](#)
- A change in output of **show chassis power** command for MX10008 and MX10016 is observed. [PR1311574](#)
- While upgrading Juniper Device Manager (JDM) there is a possibility that the jdmd process might not run after the upgrade. No errors are reported during the upgrade. [PR1313964](#)
- The **show dynamic-tunnels database summary** command might not display accurate tunnels summary when the anchor Packet Forwarding Engine line card is not up. As a workaround, use the **show dynamic-tunnels database** and **show dynamic-tunnels database terse** commands instead. [PR1314763](#)
- Alarm is raised if mixed AC PEMs are present. Changed the criteria to check whether mixed AC is present. If the PEM is AC(HIGH) first bit of pem_voltage is set and if it is AC(LOW) second bit of pem_voltage is set. If both first and second bit is set then, mixed AC is present. [PR1315577](#)
- Making changes in Traffic Load Balancer services for one instance might lead to a refresh of other existing instances. [PR1318184](#)

- According to the MACsec extended package of Network Device Protection Profile (NDPP), there needs to be an option to specify the lifetime for connectivity association keys (CAKs) based on FCS_MACSEC_EXT.4.3 (EP - NDcPP Version 1.0). This requirement indicates that there must be a start time and an end time or a time span configured for the lifetime of the CAK. In Junos OS Release 18.1R1, the end time for CAKs cannot be specified, which is a limitation. Only the start time of the various CAKs can be specified through the CLI. [PR1318543](#)
- In JDM (running on a secondary server), the jdmd process might generate a core file if guest network function (GNF) add-image is aborted by pressing CTRL+C. [PR1321803](#)
- BGP signal tunnels are always next-hop-based tunnels. The GRE tunnels created dynamically by a BGP signal are always next hop-based tunnels, even if the user has configured the static tunnels created by GRE to use the logical interface base. [PR1322941](#)
- If **commit full** is configured, the na-grpd process might restart and the streaming telemetry might disconnect. [PR1326366](#)
- When an aggregated multiservices (AMS) bundle that has a single maximum allocation bandwidth constraints model (MAM) added to the subinterfaces, the AMS interface does not recover after the subinterface has been disabled. [PR1329498](#)
- If filter is configured with the **scale-optimized** statement, then having the action pointing to traffic-class-count does not increment. [PR1334580](#)
- In some cases, the public key infrastructure (PKI) process might become busy and stop responding at the certificate hierarchy, where intermediate CA profiles are not present on the device. [PR1336733](#)
- On an MX Series platform with 100M SFP used on MIC-3D-20GE-SFP-E and MIC-3D-20GE-SFP-EH, SFP might not work if it is not from Fiberxon or Avago. [PR1344208](#)
- First packet pertaining to J-Flow Packet Forwarding Engine sensor in UDP mode is missing after a line card reboot on PORTER-R platform. [PR1344755](#)
- When community_action is specified with community_name in netconf for the **insert after** operation, you can observe a **parse error in identifier** attribute error and insertion fails. [PR1348082](#)

Infrastructure

- A file system corruption might create a kernel core file. The Routing Engine reboots with the message **ffs_blkfree: freeing free block**. [PR1028972](#)
- System with high uptime with Unigen solid-state drive (SSD) might cause watchdog panic when Junos OS Release 14.X is upgraded to Junos OS Release 15.X and later. As a workaround, reboot the system before upgrading Junos OS and avoid the "dirty" flag on your file system, which might trigger the panic. [PR1309483](#)
- To test features like nonstop active routing (NSR), the junos-panic package can be installed, and **/usr/libexec/panic** can be run from root. [PR1352217](#)

Interfaces and Chassis

- Junos OS now checks logical interface information under the aggregated Ethernet interface and prints only if it is part of the information. [PR1114110](#)
- A Junos OS upgrade involving Junos OS Release 14.2R5 and later maintenance releases and Junos OS Release 16.1 and later main releases with a connectivity fault management (CFM) configuration might cause the cfmd process to generate a core file. This is because of the presence of an old version of `/var/db/cfm.db`. [PR1281073](#)
- When you restart interface control and simultaneously take the MPC offline and bring it back online, LAG member links running LACP in slow mode might get disassociated from the LAG bundle. The issue was seen with scale configuration on DUT. The scale details are: 2800 CFM sessions, 2800 BFD sessions, 2043 BGP peers, and 3400 VRF instances. [PR1298985](#)
- CFM sessions flap on MPC5 or MPC6 with a packet-switched interface. [PR1303672](#)
- The connectivity fault management (CFM) session does not come up when configured on a logical interface whose VLAN ID matches that of the native VLAN ID configured on the physical interface. [PR1325190](#)
- When eth-oam is deactivated with scale PM configuration (under hardware-assited-pm-mode), the FPC can become unstable and can lead to generating core files. [PR1347250](#)

Layer 2 Features

- For routers equipped with T4000-FPC5-3D, MX-MPC3E-3D, MPC5E-40G10G, MPC5EQ-40G10G, MPC6E, and MX2K-MPC6E line cards, if the router is working as VPLS PE, because of the MAC aging that occurs every 5 minutes, the VPLS unicast traffic is flooded as unknown unicast every 5 minutes. [PR1148971](#)
- This issue occurs when running LACP between Juniper Networks and Cisco devices with different timers (Juniper Networks fast and Cisco slow) on both sides. On the Cisco side, it take 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](#)
- On RE-2000 running FreeBSD 10.x-based Junos OS, the following false positive CB alarms might be seen: **Aug 19 16:56:18.119 acb_pmbus_read: unable to convert voltage for CB 2 pmbus device XF ASIC A Aug 19 16:56:19.087 send: yellow alarm set, device CB 2, reason CB 2 PMBus Device Fail Aug 19 16:57:18.663 send: yellow alarm clear, device CB 2, reason CB 2 PMBus Device Fail Aug 21 22:45:04.145 acb_pmbus_read: pmbus command READ_VOUT_CMD to CB 2 XF ASIC B failed Aug 21 22:45:04.219 send: yellow alarm set, device CB 0, reason CB 2 PMBus Device Fail Aug 21 22:46:04.147 send: yellow alarm clear, device CB 0, reason CB 2 PMBus Device Fail.** [PR1298612](#)

MPLS

- When using **mpls traffic-engineering bgp-igp-both-ribs** with LDP and RSVP both enabled, constrained shortest path first (CSPF) for interdomain RSVP LSPs cannot find the exit area border router (ABR) when there are two or more such ABRs. This causes interdomain RSVP LSPs to break. RSVP LSPs within the same area are not affected. As a workaround, run RSVP only on an OSPF ABR or on an IS-IS Layer 1 or Layer 2 router and switch RSVP off on other OSPF area 0 or IS- IS Layer 2 routers; or do not use LDP at all, use only RSVP. [PR1048560](#)
- The routing protocol process (rpd) crashes when there is a GRES between the master and backup Routing Engines of different memory capabilities. For example, one Routing Engine has only enough memory to run rpd in a 32-bit mode, while the other is capable of running it in 64-bit mode. The situation might be seen in Junos OS Release 13.3 or later configured with the **auto-64-bit** statement, or in Junos OS Release 15.1 or later even without that statement configured. Under these conditions, the rpd might crash on the new master Routing Engine. As a workaround, this issue can be avoided by using the **set system processes routing force-32-bit** command. [PR1141728](#)
- With nonstop active routing (NSR), when the routing protocol process(rpd) restarts on the master Routing Engine, the process might restart on the backup Routing Engine also. [PR1282369](#)
- If you swap the binding SID between a colored and a noncolored static service request, then LSPs might cause rpd to generate a core file. [PR1310018](#)
- If there are some LSPs for which a router has a link protection available, and when a primary link failure is caused by an FPC restart, a core file might be generated. [PR1317536](#)
- When a dynamic tunnel is configured and RSVP signaling is disabled, any configuration that affects dynamic tunnels could cause the rpd process to crash. [PR1319386](#)

Platform and Infrastructure

- When using the **show | compare** method to commit, part of a configuration might be treated as noise and return a syntax error. [PR1042512](#)
- The error message **LUCHIP(5) GUMEM1[77a0]** mismatch might be seen when an MX Series MPC with the LU chip is taken offline and brought back online. [PR1221195](#)
- 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 the other events, such as spanning tree root bridge change occur. [PR1275544](#)
- With ISSU, momentary traffic loss is expected. In EVPN E-Tree, in addition to traffic loss, the known unicast frames can be flooded for around 30 seconds during ISSU before all forwarding states are restored. This issue does not affect BUM traffic. As a workaround, nonstop bridging (NSB) can be

configured using the **set protocols layer2-control nonstop-bridging** command. This reduces traffic flood to around 10 seconds in a moderate setup. [PR1275621](#)

- The apply-path prefix is not inherited under policy after commit. [PR1286987](#)
- An issue is observed with three color policer of both single-rate and two-rate types where, for a certain policer rate and burst-size combination the policer accuracy varies. This issue has been present since Junos OS Release 11.4 on all MX Series routers with MPCs or MICs. [PR1307882](#)
- Starting in Junos OS Release 17.3R1, in an EVPN setup, when performing GRES, you might see **IFBD: ifbd lookup failed** messages. [PR1317591](#)
- If a packet has three or four VLAN tags and input VLAN MAP is configured, then the corrupted packet (that is, packet with the incorrect number of VLANs) will be sent out by the Packet Forwarding Engine. [PR1321122](#)
- On an MX Series router with EVPN VXLAN, if the underlying interface for the VXLAN tunnel is LACP enabled aggregated Ethernet interface with multiple members, and one of the members is flapped, a momentary IPv4 or IPv6 inter-VNI traffic loss might be seen. [PR1326572](#)
- Traffic statistics might not match on a pseudowire subscriber interface (PS) after interface statics are cleared. [PR1328252](#)
- In an EVPN E-tree, when a customer-edge (CE) facing logical interface, which is a leaf interface, is deleted completely and added back to restore the same old state with that logical interface being part of the same EVPN, leaf-to-leaf traffic might not get blocked. [PR1330134](#)
- MPC5 - inline-ka PPP echo requests is not transmitted when anchor-point is lt-x/2/x or lt-x/3/x in the pseudowire deployment. [PR1345727](#)

Routing Protocols

- Continuous soft core files might be generated because of the **bgp-path-selection** code. The rpd process gives rise to a child process and the child process asserts to generate a core file. The cause of the issue lies with route ordering, which is corrected after the soft-assert-core file is collected, without any impact to the traffic or service. [PR815146](#)
- On MX104 routers, a scheduler-slip with high BGP route scale might be seen when you restart the router or when the OSPF protocol is disabled. [PR1203979](#)
- LDP OSPF are in in-sync state and the reason observed for this is "IGP interface down" with LDP synchronization enabled for OSPF. **user@host> show ospf interface ae100.0 extensive** Interface State Area DR ID BDR ID Nbrs ae100.0 PtToPt 0.0.0.0 0.0.0.0 0.0.0.0 1 Type: P2P, Address: 10.0.60.93, Mask: 255.255.255.252, MTU: 9100, Cost: 1050 Adj count: 1 Hello: 10, Dead: 40, ReXmit: 2, Not Stub Auth type: MD5, Active key ID: 1, Start time: 1970 Jan 1 00:00:00 UTC Protection type: None Topology default (ID 0) -> Cost: 1050 LDP sync state: in sync, for: 00:04:03, reason: IGP interface down config holdtime: infinity. Although LDP notifies OSPF that LDP sync is achieved, OSPF is not able to take note of the LDP sync notification because the OSPF neighbor was not up yet. [PR1256434](#)

- Performance degradation occurs during computation of loop free alternate (LFA) and RLFA. This issue does not impact functionality. [PR1264564](#)
- 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](#)
- When an MoFRR is configured, the routing protocol process (rpd) Packet Forwarding Engine is out of synchronization after link-flapping. [PR1284463](#)
- The routing protocol process (rpd) on both master Routing Engine and backup Routing Engine might restart continuously when having the protocols isis backup-spf-options node-link-degradation configured. [PR1299199](#)
- When route target filtering (RTF) is configured for VPN routes and multiple BGP session 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 **clear validation database** is issued back to back multiple times, you might end up with partial validation database with some validation entries missing. This eventually is recovered after up to 30 minutes (half of the record lifetime) when you do periodical full updates. [PR1326256](#)
- The issue occurs when configuring anycast and prefix segments in SPRING for IS-IS, prefix-segment index 0 is not supported, even though user is allowed to configure 0 as an index. [PR1340091](#)
- From Junos OS Release 16.1R1 and later, there might be a mismatch in the length of BGP update message between BGP main thread and I/O thread when receiving BGP updates. If this issue happens, an rpd crash might be seen. [PR1341336](#)
- There are scenarios where an application allocates and caches next hop templates. This causes the NH template cache to grow continuously. But when the application clears its local cache, then memory is freed to the NH template cache. But the NH template cache does not have code to shrink the cache and free memory back. So the NH template memory is trapped in the cache and cannot be used for other purposes. But if the same BGP routes and next hops come up again, they will reuse the templates from cache and not consume additional memory. [PR1346984](#)

Services Applications

- When one of the internal high availability queues gets corrupted, the results in mspmand generates a core file on the backup SDG. This issue occurs because sometimes different threads of mspmand might have different timestamps. [PR1291664](#)

Subscriber Access Management

- In 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](#)

- Sometimes, when a PPPoE subscriber logs in and logs out from Junos OS Release 16.1, the following messages are generated: `user@devcie> 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 **authd daemon for subscriber authentication is attempting to read private data for an underlying interface which no longer exists (-7 = SDB_DATA_NOT_FOUND)**. These messages indicate that the authd process for subscriber authentication is attempting to read the 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 because the authd process asks session database (SDB) for a record that no longer exists. [PR1236211](#)

VPNs

- VLAN-CCC logical interface for Layer 2 circuit remains in CCC-down state upon Layer 2 circuit to EVPN-VPWS service change unless it is deactivated and re-activated manually. [PR1312043](#)

SEE ALSO

[New and Changed Features | 90](#)

[Changes in Behavior and Syntax | 110](#)

[Known Behavior | 115](#)

[Resolved Issues | 128](#)

[Documentation Updates | 154](#)

[Migration, Upgrade, and Downgrade Instructions | 155](#)

[Product Compatibility | 162](#)

Resolved Issues

IN THIS SECTION

● [Resolved Issues: 18.1R2 | 129](#)

● [Resolved Issues: 18.1R1 | 136](#)

This section lists the issues fixed in the Junos OS 18.1R2 Release for MX Series routers.

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

Resolved Issues: 18.1R2

Class of Service (CoS)

- CoS wildcard configuration is applied incorrectly when the router restarts. [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 when **excess-bandwidth-share** is configured. [PR1348698](#)

EVPN

- On deactivated ESI for PS at physical interface level, routing protocol process crashes and generates a core file for EVPN VPWS PWHT. [PR1332652](#)
- In an EVPN and NSR environment, the routing protocol process (rpd) crash and generates a core file on backup Routing Engine for any configuration changes on master Routing Engine. [PR1336881](#)
- The rpd process might crash when executing CLI command **show route evpn-ethernet-tag-id**. [PR1337506](#)
- In an EVPN and VXLAN environment, Packet Forwarding Engine crashes when BFD and VTEP flap. [PR1339084](#)
- Bring the IRB logical interface UP, even if L2 interfaces are absent but IM next hop is present. [PR1340723](#)
- The rpd might crash if the IRB interface and routing instance are deleted together in the same commit. [PR1345519](#)

Forwarding and Sampling

- The error messages about dfw_gencfg_handler might be seen during unified ISSU. [PR1323795](#)
- DHCP service crashes after EX9251 switch is set to factory default by zeroize [PR1329682](#)
- The error logical interface under VPLS might be blocked after MAC moves if the logical interfaces are on the same physical interface. [PR1335880](#)
- The l2ald crashes when a duplicate MAC is learnt by two different interfaces. [PR1338688](#)
- Commit failed when attempting to delete any demux0 unit numbers which are greater or equal to 1000000000. [PR1348587](#)

General Routing

- Memory leak is causing the rpd crash. [PR1052614](#)
- Unexpected MobileNext Gateway Activation license alarms when TDF gateway is configured. [PR1162518](#)

- SNMP trap sent for "PEM Input failure" alarm is not generated when a single input feed fails on MX960. [PR1189641](#)
- High priority fabric drops from MPC7E towards MPC3E next-generation. [PR1207417](#)
- High priority fabric drops from MPC7E towards MPC3E next-generation. [PR1226804](#)
- The error log messages **cc_mic_irq_status: CC_MIC(5/2) irq_status(0x1d) does not match irq_mask(0x20), enable(0x20), latch(0x1d)** are seen continuously for "MIC-3D-4OC3OC12-1OC48". [PR1231084](#)
- BSYS logs GNF owned pics does not support power-off configuration at commit when no such configuration is present. [PR1281604](#)
- On EVPN or VXLAN, inter-vrf traffic blackhole is seen after the routing is restarted repeatedly on redundant gateways. [PR1289091](#)
- The log message about shutdown time is incorrect when system exceeds chassis over temperature limit. [PR1298414](#)
- Utilization of **commit check** just after setting master-password can trigger improper decoding of configuration secrets. [PR1310764](#)
- The incorrect error number might be reported for syslog messages with a prefix of **%DAEMON-3-RPD_KRT_Q_RETRIES**. [PR1310812](#)
- The transient error **hawkeye alarmd** are observed on MX240, MX480, and MX960 Series routers. [PR1312336](#)
- The MPC with specific failure hardware might impact other MPCs in same chassis. [PR1319560](#)
- The rpd might crash when two next hops are installed with the same next hop index. [PR1322535](#)
- MS-MIC interface logical interfaces remain down after many offline or online iterations. [PR1322854](#)
- CLI command **request vmhost halt routing-engine other** does not halt the backup Routing Engine. [PR1323546](#)
- The snmp interface filter does not work when "interface-mib" is part of dynamic-profile. [PR1324573](#)
- Constant logging of **fm_feacap_sys_feature_get:Attribute DB init not yet done, reading from pvid (id: 18)**. [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 do not rewrite 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 configuration. [PR1329931](#)
- **Too many supplies missing in lower and upper zone** alarm flaps (set/clear) every 20 seconds if a zone does not have minute required PSMs. [PR1330720](#)

- In rare cases, a highly scaled node-slicing Guest Network Function (GNF) might fail to complete NSR replication after a NSR switch over. This is true even if the GNF is confirmed NSR ready before the switch occurs. [PR1331145](#)
- Two subscribers cannot reach the online state at the same time if they have an identical frame-route attribute value. [PR1334311](#)
- Hitless key-chain rollover feature has limitations when used on MIC-MACSEC-MRATE. [PR1335644](#)
- The MAC_STUCK might be seen on MS-MPC or MS-MIC linecards. [PR1335956](#)
- 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](#)
- FPC temperature might mismatch for MPC6, MPC8, and MPC9 on MX2000 platform. [PR1339077](#)
- DDoS counters for OSPF might not increase. [PR1339364](#)
- CLI shows CB states online after pressing RCB offline button for more that four seconds. [PR1340431](#)
- VRRP sticks in master on upgrade or cold boot. [PR1341044](#)
- When discard interfaces are configured with IGMPv3, KRT queue gets stuck while deleting multicast next hop (MCNH) with error **EPERM -- Jtree walk in progress**. [PR1342032](#)
- The FPC is marked as down and stay down on the MX150 platform causing service effecting loss of traffic. [PR1343170](#)
- In MPLS or RSVP environment, LSP might stick in Dn state with **Record route: <self> ...incomplete**. [PR1343289](#)
- Queue counters are not getting displayed in the interface details for PORTER-R once the system reboots. [PR1343306](#)
- Support required for **show system resource-monitor subscribers-limit chassis extensive in Summit**. [PR1343853](#)
- Stout card crash and generates a core file when DHCPv6 on static VLAN logout. [PR1343965](#)
- The l2cpd process might generate a core file on executing **l2cpd_ifbd_attach** command (where ifbd=0x98914c0, vlan_id=1, line_vid=1) after disabling mc-ae on qfx10002-60c {default vlan-scenario} which is getting hit where delete is missed by l2cpd because it uses Sync socket read when it starts. [PR1344983](#)
- The routing protocol process (rpd) crash might be seen if the **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 is changed from JNP10003-RE1 to RE-S-1600x8. [PR1346054](#)
- New PPPoE users might fail to login. [PR1346226](#)
- VCCP-ADJDOWN detection is delayed on VC-Bm when deleting one VCP link on VC-Mm. [PR1346328](#)

- The twice-napt-44 sessions are not synchronizing to backup SDG with **stateful sync** configured. [PR1347086](#)
- Remove libstdc++ dependency on hypervisor to install JDM rpm or deb package. [PR1347921](#)
- 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](#)
- The **get config** configuration statement for hidden choices is not working with ODL controller. [PR1348503](#)
- MACsec ACK validation is added for boundary condition check and invalid values (entering '0x0' or '0x0000000000000000' as an error). [PR1348642](#)
- Chassisd memory leak issue is seen on MX10003 and MX204 platform and it might eventually switchover Routing Engine and crash. [PR1348753](#)
- MGD core files are generated because of the issue in nsindb infrastructure. [PR1349288](#)
- The error message **Major PEM 0 Input Failure** might be observed for DC PEM. [PR1349179](#)
- Access internal routes remain even after AIU is completed. [PR1350401](#)
- The MTU value for subscriber's interface might be programmed incorrectly if the statements **routing-services** or **protocol pim** is configured in dynamic-profile. [PR1350535](#)
- The subinfo process might crash when executing **show subscribers address <> extensive** for a DHCPv6 address. [PR1350883](#)
- Dynamic physical interface creation fails when the SFP optic is plugged in MX150. [PR1351387](#)
- Node virtualization MSE after reinstalling one JDM server complains pull configuration failed, fallback to push configuration method. [PR1352503](#)
- On MX Series routers show chassis fpc errors does not show errors on GNF systems. [PR1352705](#)

High Availability (HA) and Resiliency

- 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](#)

Interfaces and Chassis

- L2TP subscribers might not be cleared if the access-internal routes fail to install. [PR1298160](#)
- MPC CPU might reach 100 percent when **otn ufec** statement is configured. [PR1311154](#)
- No route to IP address from directly connected route. [PR1318282](#)
- 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](#)
- The cfmd process core files are generated. [PR1329779](#)
- The dcd process might crash because of the memory leak and causes commit failure. [PR1331185](#)

Layer 2 Ethernet Services

- The memory leak might occur in l2cpd if the l2-learning process is disabled. [PR1336720](#)
- DHCP client is not able to connect if VLAN was modified on aggregated Ethernet interface associated with the IRB. [PR1347115](#)
- Restart FPC which host micro-bfd link might cause lacp to generate a core file. [PR1353597](#)

Layer 2 Features

- The rpd process memory leak is observed upon any changes in VPLS configuration like deleting or re-adding VPLS interfaces. [PR1335914](#)

MPLS

- Whenever there is a decrease in the statistics value across an LSP, the mplsLspInfoAggrOctets value take two intervals to get updated. [PR1342486](#)
- An LDP label is generated for serial interface subnet route unexpectedly. [PR1346541](#)
- In a very rare scenario, rpd might crash when LDP fails to allocate self-id for the P2MP FEC. [PR1349224](#)
- The rpd crash might happen in RSVP setup-protection scenario. [PR1349036](#)

Network Management and Monitoring

- The eventd process fails to startup with syslog configuration. [PR1353364](#)
- SNMP stops or becomes very slow after a very long period of time. [PR1328455](#)

Platform and Infrastructure

- MX204 performance degrades when using firewall filter with sampling action. [PR1303529](#)
- VPLS instance fails to learn MAC addresses upon pseudowire switchover. [PR1316459](#)
- 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 TCP dump filter might not work in egress direction on PS and lt logical interfaces. [PR1329665](#)
- Commit might fail with error reading from commit script handler. **commit script failure.** [PR1335349](#)
- While downgrading MX Series router from a later release, the router goes into amnesiac state. [PR1341650](#)
- Configuring the same DHCP server in different routing-instances is not supported in DHCP relay scenario. [PR1342019](#)
- Commit error on configuring same vlan-id on different logical interface of the same lt physical interface when **ethernet-bridge encapsulation** is configured. [PR1342229](#)

- Route corruption in Packet Forwarding Engine with **connectivity-fault-management** enabled for Layer 2 circuit. [PR1342881](#)
- ZTP is not supported for vmhost images on next generation Routing Engines on the MX Series platforms. [PR1343338](#)
- IPv4 GRPS traffic over aggregated Ethernet interface might be affected if enhanced hash key **gtp-tunnel-endpoint-identifier** is configured. [PR1347435](#)
- On MX Series routers, in an EVPN-VXLAN 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](#)
- ICMP error messages are not generated if 'don't fragment' packets exceed the MTU of the multiservice interface. [PR1349503](#)
- The CLI commands **system ddos-protection protocols unclassified** are missing on MX2020. [PR1349782](#)
- Suspect memory leak in chassisd. [PR1353111](#)

Routing Policy and Firewall Filters

- Access-internal route might fail to be leaked between routing instances when "from instance" is configured in the policy. [PR1339689](#)

Routing Protocols

- BGP extended communities with sub-type 4 erroneously displayed at LINK_BANDWIDTH. [PR1216696](#)
- The routing protocol process (rpd) generates a core file in the ASBR when BGP is deactivated in the ASBR before all stale labels have been cleaned up. [PR1233893](#)
- BGP traceoption logs are still written when it is deactivated. [PR1307690](#)
- In IS-IS and IPv6 scenario, rpd might crash when the neighbor router is restarted and causes routes to churn. [PR1312325](#)
- 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](#)
- Traffic might get silently dropped and discarded temporarily when BGP GR is triggered and the direct interface flap. [PR1319631](#)
- When tracing BGP routes that contain the DF election community, BGP communities after this community might not display properly. [PR1323596](#)
- Manual GRES with MX Series Virtual Chassis results in some packet loss on core facing interfaces. [PR1329986](#)
- The LDP route in inet.3 is missing when both OSPF rLFA and LFA protections are available and rejected by backup selection policy. [PR1333198](#)

- In TOMCAT, IGMP joins are not processed with **passive allow-receive** statement configured on IGMP interface. [PR1334913](#)
- The routing protocol process (rpd) generates a core file during delete and restore of BGP configuration. [PR1338567](#)
- Changes to the displayed value of AIGP is seen when **show route ... extensive** command is executed. [PR1342139](#)
- Traffic black-hole might be seen if local DUT receives BFD-down. [PR1342328](#)
- The rpd might crash when BGP flaps. [PR1342481](#)
- The rpd might crash if a route for RPF uses a qualified-next-hop. [PR1348550](#)
- The routing protocol process (rpd) might crash while restarting routing or deactivating IS-IS. [PR1348607](#)
- **source-as community** is not appended to rendezvous point (RP). A display issue is observed in **show route detail** command output. [PR1353210](#)

Services Applications

- SNMP MIBs do not yield data related to sp- interfaces. [PR1318339](#)
- Crash at `../src/junos/lib/libjuniper/mgmt-sock/mgmt_sock_select_info.c:35`. [PR1337406](#)
- 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](#)

Software Installation and Upgrade

- New versions of Junos OS does not have the tool for accessing aux port - `/usr/libexec/interposer`. [PR1329843](#)

Subscriber Access Management

- The L2TP LAC might drop packets that have incorrect payload length while sending packets to the LNS. [PR1315009](#)
- The multiple RADIUS servers having different dynamic request port is not supported. [PR1330802](#)
- Traffic drops on the MX Series router LNS because of software error or unknown family exception when traffic is destined to or coming from MLPPP subscriber if **routing-services** configuration statement is present in the dynamic-profile used by this subscriber. [PR1335276](#)
- The subscriber might get stuck in terminated state when JSRC synchronize state get stuck in "FULL-SYNC in progress". [PR1337729](#)
- MX Series router is sending IPv6 RA and the DHCPv6 advertisements before IPCPv6 Ack from CPE. [PR1344472](#)
- The ancpd process might generate a core file when clearing ancp subscribers in a scaled scenario when **enhanced-ip** is configured. [PR1344805](#)

- The bbe-smgd process might crash if there are 65535 L2TP sessions in a single L2TP tunnel. [PR1346715](#)
- Subscriber might experience SDB DOWN event and drop the clients' connections when issuing **show subscribers** command. [PR1336388](#)
- LNS subscribers on aggregated-inline service scale impacted. [PR1341659](#)
- **AC system error** counter in **show pppoe statistics** does not work. [PR1346231](#)
- The pfd process consumes 80 to 90 percent CPU running subscriber management on PPC based routers. [PR1351203](#)

VPNs

- 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](#)
- The routing protocol process (rpd) crashes after committing interface related parameters (for example, MTU change, VRF RD/RT, QOS) on PS interface with vlan-ccc encapsulation and no vlan-id. [PR1329880](#)
- The routing protocol process (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 while changing the I2circuit virtual-circuit-id in an NSR scenario. [PR1345949](#)

Resolved Issues: 18.1R1

Application Layer Gateways (ALGs)

- IKEv2 negotiation might fail with IKE ESP ALG enabled in IKEv2 redirection scenario. [PR1329611](#)

EVPN

- EVPN traffic does not map to a specific LSP in the core. [PR1281415](#)
- BGP route refresh request might not be sent when the route target is modified. [PR1300332](#)
- Split horizon label is not allocated when the configuration of ESI is switched from **single-active** to **all-active**. [PR1307056](#)
- Discard EVPN route is installed on local PE device when the connection flaps on a remote PE device in a multihome EVPN topology. [PR1321125](#)
- FPC might stop functioning properly while deleting the VPLS configuration having the **no-tunnel-service** command enabled from the routing instance. [PR1324830](#)

- The core link flapping might result in an inconsistent global MAC count. [PR1328956](#)
- On restarting the router using **restart routing**, the rpd process generates a core file in provider edge (PE) router that has EVPN-VXLAN configuration. [PR1333331](#)

Forwarding and Sampling

- When subscriber services that are enabled for interim volume accounting goes down, the pfd process rarely generates a core file with the backtrace pfd_timer_manager_remove_serv_id. [PR1296969](#)
- There is a memory leak on mib2d when firewall MIBs are polled. [PR1302553](#)
- The remote CE1 MAC address might take along time to meaning not clear. [PR1304866](#)
- In a subscriber management environment, when the **show firewall templates-in-use** command is executed, dfwd process might crash during the execution if a CLI session disconnects before the complete output of this command is received. [PR1305284](#)
- ACCT_FORK_LIMIT_EXCEEDED log level is an error even when backup-on-failure feature is enabled for accounting files. [PR1306846](#)
- Second archive site in the accounting file configuration is not used when the first one uses SFTP protocol and is not reachable. [PR1311749](#)
- Accounting files with no records might be unexpectedly uploaded to the archive site. [PR1313895](#)
- The log message **dfwinfo: tvptest:dfwi_counter_output policer_byte_count support 0** might be noticed when issuing **show firewall** related command. These logs are harmless and intended for debug purpose.. [PR1315730](#)
- The commit might fail if the **next-hop learning** configuration statement is enabled for J-Flow v9. [PR1316349](#)
- The FPC CPU might reach 100 percent constantly when the shared bandwidth policer is configured. [PR1320349](#)
- Some firewall filter counters might not be created in SNMP. [PR1335828](#)

General Routing

- Maintenance association end-points (MEPs) persist to generate continuity check message (CCM) frames, after they are deleted from protocols OAM Ethernet CFM stanza. [PR1107542](#)
- Memory leak is seen on Layer 3 VPN configuration commit for L3VPN scaling test. [PR1115686](#)
- No warning is raised when the bridge family is configured with an interface-mode trunk but without VLAN tagging or flexible VLAN tagging. [PR1154024](#)
- Ksyncd process might not respond because of transient replication errors between Routing Engines. [PR1161487](#)
- Stale VBF states occur without SDB sessions. [PR1204369](#)

- Unable to deregister sub error (131072) for error (0x1b0001) for module MIC error messages seen on MPC5E card. [PR1221337](#)
- Changing the virtual switch interface type from IRB to regular bridge interfaces under the OpenFlow protocol are removed. The OpenFlow process (daemon) fails to program any flows. [PR1234141](#)
- The **multicast-replication** setting cannot be reflected in the redundancy environment after both Routing Engines are rebooted. [PR1240524](#)
- In a BGP and MPLS scenario, if the next hop type of label route is indirect, disabling and enabling the **family mpls** configuration of the next-hop interface might cause the route to go into a dead state. [PR1242589](#)
- The **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 restarts. [PR1243364](#)
- Prolonged flow control core file is observed for the TFTP ALG traffic (10K simulated users). [PR1255973](#)
- When you plug in an SFP or SFP+ transceiver or remove it from any of the supported ports on an MX150, the ge-0/0/0 interface goes down and cannot be used. [PR1259112](#)
- GNF sometimes resets its MPC type 9 at NSR at a high scale. [PR1259910](#)
- The virtual MX Series router with FPC generates a core file - panic (format_string=format_string@entry=0x9e509c4 "Thread %s attempted to %s with irq priority at %d\n"). [PR1263117](#)
- Monitoring FPC temperature is not applicable on MX1RU platform, because MX1RU is a single board design with logical FPC. [PR1263315](#)
- On MX Series, the **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 might cause the SIP ALG to generate a core file. [PR1268891](#)
- The load-based throttling is not enabled. [PR1271739](#)
- Aggregated Ethernet incorrect counters for output packets on child links for ae0 interface when configured with new feature 'revertive'. [PR1273983](#)
- On an MX104 platform with GRES enabled, the chassis network-services might not get set as "Enhanced-IP". [PR1279339](#)
- The jfirmware upgrade support is not available for Routing Engine BIOS. [PR1281050](#)
- BSYS logs GNF owned pics does not support power-off configuration at commit when no such configuration is present. [PR1281604](#)
- The kernel crash might happen in a rare corner case. [PR1282573](#)
- In a specific CE device environment in which asynchronous-notification is used, when the link between the PE and CE devices goes up, the L2 circuit flaps repeatedly. [PR1282875](#)

- The total number of corrected single-bit errors from HMC [x] exceeds the threshold value of 32. [PR1285315](#)
- LC, PFH, and Packet Forwarding Engine interfaces do not come up on the RE1. [PR1285606](#)
- A missing statement “Shared bandwidth policer not supported for interface ge-x/x/x” is noticed when a commit is unsuccessful in Junos OS Release 16.1R3. [PR1286330](#)
- During unified ISSU (FRU upgrade) micro BFD flapping is observed. [PR1288433](#)
- The interfaces might go to a down state after performing GRES. [PR1289493](#)
- The **request system zeroize** command deletes the **/var/db/scripts** directory, which is not re-created until the next USB or netboot recovery. [PR1289692](#)
- **jnxContainersType** MIB is not displayed for MX Series MICs and PICs as correctly as it is displayed on other Juniper Network platforms. [PR1289778](#)
- Incorrect temperature is displayed for MPC5 and MPC7 in the **show chassis fpc** command output. [PR1290771](#)
- The traffic traversing a label-switched path (LSP) with entropy label might get dropped after the bypass path goes down. [PR1291036](#)
- The routing protocol process (rpd) might generate a core file while it is restarted from the CLI. [PR1291110](#)
- The L2TP ICCN fast retransmission occurs after tunnels go down. [PR1291557](#)
- When GRES is enabled, restarting the chassisd process results in FPC restarting multiple times. [PR1293314](#)
- On an MPC6E, with inline flow monitoring enabled, the flow export rate remains less as compared to the configured export rate. [PR1294296](#)
- During PPPoE subscriber login, errors such as [**vbf_flow_src_lookup_enabled**] and [**failed to find iff structure, ifl**] were seen on the FPC. [PR1294710](#)
- The KRT queue might get stuck with the error **RPD_KRT_Q_RETRIES: chain nexthop add: Unknown error: 0**. [PR1295756](#)
- A [**First_Net**] commit error is thrown when you try to commit a configuration with the applied groups. [PR1298649](#)
- MX Series BNG does not respond to PADI after GRES on some ports or VLANs. [PR1298890](#)
- In certain conditions, the maximum count is reached, if a limit configured by a subscriber does not allow a second family of DHCP dual stack. [PR1298924](#)
- Software enhancements are made to AC NON-HC PEM that suppresses the I2C bus errors for PEM. [PR1299284](#)
- The asynchronous-notification feature cannot be implemented properly in a circuit that has MIC-3D-20GE-SFP-E or Tri Rate Copper SFP(740-013111). [PR1299574](#)
- ICMP or ICMPv6 error messages might be discarded while getting forwarded through an AMS interface. [PR1301188](#)

- A configured logical interface might not be created correctly after the configuration is committed. [PR1301823](#)
- In Junos Telemetry Interface (JTI) setup, the payload MTU might be much less than 16 KB when subscribing to a component sensor. [PR1301835](#)
- Duplicate keys are no longer exported by the physical interface related to Packet Forwarding Engine; these are only exported by MIB2D. [PR1301858](#)
- The rpd process might crash when NSR is enabled and the routing-instance specific configurations are committed. [PR1301986](#)
- Continuous interface flapping might lead to unwanted resetting of the MIC. [PR1302246](#)
- The rpd process might crash when the **vrf-propagate-ttl** and **no-vrf-propagate-ttl** configuration statements are toggled. [PR1302504](#)
- The **chassisd.core-tarball.0.tgz** file is found during unified ISSU is aborted during the upgrade of a FRU. [PR1303086](#)
- Incorrect MTU might be seen on PPP interfaces when PPP MTU is not defined in the dynamic profile. [PR1303175](#)
- The inline-ka PPP echo requests are no longer generated for aggregated Ethernet interfaces. [PR1303249](#)
- The **request auto-configuration reconnect-pending** command is no longer available. [PR1303336](#)
- Blocking PPPoE or DHCP to initiate VLAN autosensing when the VLAN-OOB is in pending state. [PR1303338](#)
- Fan speed changes frequently on MX Series chassis. [PR1303459](#)
- When MPLS LSP self-ping is enabled (self-ping is enabled by default), the kernel might panic, generating the error message **Fatal trap 12: page fault while in kernel mode**. [PR1303798](#)
- MX Series MIB polling returns a value that has **sdg**. Polling result should include **svc** generic value. [PR1303848](#)
- Truncated output appears for the **show pppoe lockout** command. [PR1304016](#)
- When either a MPC6E or SFB2 restarts, you might see link errors and training failure between fabric planes. [PR1304095](#)
- Effective rate of E3 in framed mode is limited to 30 Mbps on certain channelized MICs. [PR1304344](#)
- The RPF check strict mode causes traffic drop in the next-generation subscriber management release. [PR1304696](#)
- On an MX2000 with MPC9E and SFB2 installed, a certain high amount of traffic volume might cause traffic drops and generate cell underflow messages. [PR1304801](#)
- 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](#)
- The MX Series router sends immediate-interim reports for the services pushed by SRC. [PR1305425](#)

- When traceoptions are enabled on 32-bit Junos OS, the rpd process might generate core files. [PR1305440](#)
- JET daemonize application gets respawned even on normal exit. [PR1305615](#)
- The LIBJNX_REPLICATE_RCP_ERROR message is seen in the syslog when a backup Routing Engine is not present. [PR1305660](#)
- L2BSA subscriber's connection attempts failed with VLAN **profile-request-error**. [PR1305962](#)
- The network FPC command **start shell Packet Forwarding Engine** is not working on MX960. [PR1306236](#)
- L2BSA subscribers are not able to connect, and no new ANCP session get established during the RADIUS disaster backup procedure. [PR1306872](#)
- The smihelperd process generates core files when SNMP is polling for JUNIPER-SUBSCRIBER-MIB::jnxSubscriberGeneral.7.0. [PR1306966](#)
- The kmd process error **UI_DBASE_OPEN_FAILED** is seen because of too many open files. [PR1308380](#)
- License is lost during Routing Engine switchover in scale-subscriber scenario. [PR1308620](#)
- CoS applied to a subscriber DEMUX logical interface does not work. [PR1308671](#)
- All the MICs on one MPC, with PWHT subscribers configured, might go offline during the restart of an MPC installed 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 timestamp values are found when RADIUS accounting stops packets. [PR1309212](#)
- On MX2020 and MX2010, after a smooth upgrade from SFB to SFB2, if one plane or SFB is restarted, the link training fails between those planes and the MPC6 line-cards. [PR1309309](#)
- When the Routing Engine mastership is switched, the bbe-mibd process might generate a core file. [PR1309341](#)
- The first access-request fails for L2BSA subscribers when the MTU of LACP aggregated Ethernet A10NSP interface. [PR1309599](#)
- The RPT BBE REGRESSIONS: DHCP client is stuck in selecting state while verifying untagged DHCP subscribers after modifying router configuration. [PR1309730](#)
- DT_BNG: 9000 out of 10,000 terminated subscribers go down during the unified ISSU from Junos OS Release 16.1-20170922_161_r4_s 6.0 to Junos OS Release 17.3-20170923.0. [PR1309983](#)
- In the next-generation subscriber management release, memory leak is seen for the bbe-smgd process after the address pool is deleted or added. [PR1310038](#)
- The MS-MIC or MS-MPC might experience a high memory utilization in the subscriber management scenario. [PR1310064](#)
- **SPD_CONN_OPEN_FAILURE** and **SPC_CONN_FAILURE** log messages are seen in the log for SI interfaces when SNMP walk is on service PIC NAT OIDs. [PR1310081](#)

- The `krt_junos_sanity_check_ctrl_resp`: rtsock request finally succeeded after error 16 syslog message in Junos OS Release 17.1R1.8. [PR1310678](#)
- The local IPv6 interface in the NDRA prefix is not removed from the service interface when the subscriber dual-stack session is removed. [PR1310752](#)
- Utilization of **commit check** while setting master-password might trigger improper decoding of configuration secrets. [PR1310764](#)
- After the base systems reboot, the rpd process is unresponsive on one or more GNFs. [PR1310765](#)
- Bad Junos Telemetry Interface (JTI) packaging for MPLS sensor. [PR1310932](#)
- The FPC memory might get exhausted with SHEAF leak messages seen in the syslog. [PR1311949](#)
- The routing protocol process generates a core file when multiple session flaps are observed on scale setup. [PR1312169](#)
- Incorrect incrementing of the counter at the PPPoE session logical interface (IFL) might lead to incorrect Acct-input-packets value and incorrect Acct-input-octets value in accounting packet. [PR1312998](#)
- False overtemperature SNMP trap could be seen when using MPC5, MPC6, MPC7, MPC8, and MPC9. [PR1313391](#)
- MX-VC: BNG: IPv6 router-solicit packets are dropped in non-default RI, but for the default RI the packets are not dropped. [PR1313722](#)
- The **show version detail** command output displays severe error log messages **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 and SFW sessions. [PR1314070](#)
- The JDM link is incorrectly shown to be up when the underlying physical link is down. [PR1314180](#)
- The **show version detail | no-more** CLI hangs for more than 120 seconds on master Routing Engine and more than 60 seconds on 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 stops responding in an multicast-only fast reroute (MoFRR) scenario. [PR1314711](#)
- In MPC7E, the **IR-mode** configuration statement fails to commit. [PR1314755](#)
- An RPC error is observed when you try to commit the **system services subscriber-management enable** statement through NETCONF. [PR1314968](#)
- MPC might crash after unified ISSU is performed multiple times. [PR1314982](#)
- The output of the **show version detail** command displays the severe error log message **mobiled: main Neither BNG LIC nor JMOBILE package is present, exit mobiled**. [PR1315430](#)
- The output of the **show version detail** command displays the severe error log message **main: name: SRD ret: 0**. [PR1315436](#)

- The output of the **show subscribers summary port** command does not display the correct output when subscribers are connected over a pseudowire. [PR1315659](#)
- An rpd core file is generated when the **show route inetcolor.0** command is executed. [PR1316078](#)
- On MX Series routers, the fan speed might frequently keep changing between normal and full. [PR1316192](#)
- The **show auto-configuration out-of-band** CLI command shows the same output for different statements. [PR1316661](#)
- The demux interface sends neighbor solicitation with the source link MAC address that comprises zeros: 00:00:00:00:00:00. [PR1316767](#)
- Traffic Load Balancer (TLB) traffic statistics counters do not get updated in Junos OS Release 18.1. [PR1317077](#)
- A few issues are seen in the output of the **show configuration display JSON** command for example, the alphanumeric values do not match the JSON output. [PR1317223](#)
- Linux-based microkernel might panic because of concurrent update of mutable objects. [PR1317961](#)
- CoA shaping rate is not applied successfully after the unified ISSU from Junos OS Release 15.1R6.7 to Junos OS Release 16.1R6.2. [PR1318319](#)
- The rpd process might stop responding after link flapping is experienced on an adjacent router. [PR1318476](#)
- The bbe-smgd process might stop responding after GRES is performed. [PR1318528](#)
- Changed text reported in **show chassis hardware** for CFP2-DCO optical transceivers. [PR1318901](#)
- MS-MPC or MS-MIC might crash after a new IPsec tunnel is added. [PR1318932](#)
- Kernel core is seen when more than 256 routing instances are created. [PR1319781](#)
- In some cases after multiple NSR switchovers replication might not complete for BGP, LDP, or RIP. [PR1319784](#)
- Loading an xmlproxyd YANG module file bounces the telemetry sessions. [PR1320211](#)
- Chassis MIB SNMP OIDs for VC-B member chassis are not available after a unified ISSU of MX Series Virtual Chassis. [PR1320370](#)
- PPP inline keepalive does not work as expected when the CPE aborts the subscriber session. [PR1320880](#)
- If OpenConfig is used for telemetry and BGP data is being streamed, the rpd stop responding when the configuration that removes a BGP peer from group is committed. [PR1320900](#)
- The MX Series router sends IPv6 RA and the DHCPv6 advertisements before IPCPv6 Ack from the CPE. [PR1321064](#)
- The bbe-smgd process generates a core file after massive clients logs out and logs in a PPPoE dual stack subscriber scenario. [PR1321468](#)
- A CoA-NAK with **Error-Cause = Invalid-Request** is sent back to the RADIUS server when a drop policy is applied under **radius-flow-tap** in an L2TP subscriber scenario. [PR1321492](#)

- In Junos Node Slicing, the hierarchy of **show system schema module** is broken. [PR1321682](#)
- The commit operation might get stuck after commit check is performed. [PR1322431](#)
- The rpd process might crash when OpenConfig package is upgraded with JT1 streaming data in the background. [PR1322553](#)
- MS-MIC logical interfaces remain down after many iterations of taking them offline and bringing them back online. [PR1322854](#)
- When RPT BBE regression test is performed, an incorrect output is observed while verifying the **show subscribers client-type vlan subscriber-state active logical-system default routing-instance default** command. [PR1322907](#)
- The **show system subscriber-management route routing-instance <xxx>** command shows unexpected outputs. [PR1323279](#)
- The CLI command **request vmhost halt routing-engine other** does not halt the backup Routing Engine. [PR1323546](#)
- After successive flaps on core interfaces in AA Multihoming EVPN VXLAN, some race conditions might trigger constant high CPU on backup Routing Engine, where rpd shows very high CPU. [PR1334235](#)
- The subscriber might fail to log-in after the interface is deactivated and re-activated. [PR1324446](#)
- Memory leakage might be seen in the mosquito-nossl daemon in an MQTT scenario. [PR1324531](#)
- For payload prefix resolved through SRTE **color multi-path protocol-nexthop**, initially route resolution works correctly; thereafter because of some network change events, the SRTE multipath next hop updates might get stuck in the async-ket IO thread. To recover, flap the corresponding BGP session. [PR1324669](#)
- SNMP values do not increase monolithically. [PR1325128](#)
- Approximately 3 percent of Packet Forwarding Engine forwarding capacity might be seen on the XM chip when temperature of the chip is higher than 67 degrees Celsius. [PR1325271](#)
- MACsec session might fail to establish on the MX10003. [PR1325331](#)
- On a SIP ALG, core files are generated and its memory is exhausted. [PR1326394](#)
- MACSec MKA transmits the upper limit of the interval. [PR1326526](#)
- In MX Series, BNG CoS service object is not deleted properly for TCP and scheduler. [PR1326853](#)
- A minor alarm "LCM Peer Connection un-stable" is observed on MX150. [PR1328119](#)
- In JDI BBE, when regression test is performed for **show class-of-service interface demux0 <demux-interface>**, "Adjustment overhead-accounting mode" does not provide the expected output. [PR1329212](#)
- The CLI command **show services nat mappings address-pooling-paired** times out and fails. [PR1330207](#)
- All the packets might get dropped if one route is advertised by BGP when a session is established through the subscriber interface. [PR1330737](#)

- FPC wedge with fragmented packets on LSQ interface - PT1: Head and Tail out of synchronization. [PR1330998](#)
- The bbe-smgd process might crash after the **clear ancp access-loop circuit-id <circuit-id>** command is run. [PR1332096](#)
- Inaccurate J-Flow records might be seen in the output interface and next hop. [PR1332666](#)
- On MX150 platform, when **set chassis alarm management-ethernet link-down ignore** is set, FPC mgmt 0 interface alarm is not ignored. [PR1332799](#)
- The subinfo process might crash and it might cause the PPPoE subscribers to get disconnected. [PR1333265](#)
- MPC8E or MPC9E report high temperature alarms and fan speed moving continuous through full and normal speed iterations. [PR1334750](#)
- The UID limit is reached in a large-scale subscriber scenario. [PR1334886](#)
- When using **show subscribers**, and when the FPC number has two digits, the interface and IPv6 address that get connected together for DHCPv6 prefix delegation (PD). [PR1334904](#)
- The any-any option cannot be configured in a traffic selector for either IPv4 or IPv6 traffic. [PR1334966](#)
- JET application might not respawn after a normal exiting. [PR1336107](#)
- BBE-SMGD process might generate a core file while configuring CoS **ifl-set**. [PR1336852](#)
- 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](#)
- CM2.0 configuration is hidden in Junos OS 18.1 Release because of systest resources. However, the **show chassis fpc** error has changed the output. [PR1337467](#)
- IPsec VPN, session and service set sensor protocol files are being added to the Junos Telemetry Interface packaging. [PR1339883](#)
- MAC address of multiple interfaces are found to be duplicate. [PR1345882](#)
- The FPC temperature mismatch is seen between **show chassis fpc** and **show chassis fpc detail** for MPC6, MPC8, and MPC9 on MX2K platform. [PR1339077](#)

High Availability (HA) and Resiliency

- After server links flap, the GNFs associated with the ports on the Control Board shows this status message **Switchover Status: Not Ready**. [PR1306395](#)

Infrastructure

- The syscalltrace.sh file might create a huge output file that can cause the router to run out of storage space. [PR1306986](#)
- Cleanup at thread exit causes memory leak. [PR1328273](#)

Interfaces and Chassis

- On MX240, MX480, and MX960, IPv6 neighborship is not created on the IRB interface. [PR1198482](#)
- The output value is incorrect when you query the optical power of OTN interfaces in the router. [PR1216153](#)
- Rate-Limit -dropped packets are not displayed by [**show interfaces <ifl or-> detail/extensive**] commands. [PR1249164](#)
- The monitoring interface on aggregated Ethernet logical interfaces displays an incorrect BPS value compared to that displayed on **show interface** command output. [PR1283831](#)
- The **delay-buffer-rate** command with an absolute value is allowed on an inline LSQ interface. [PR1300281](#)
- Some CFM sessions do not come up after router with MPC8/9E line cards are rebooted with the scaled configuration. [PR1300515](#)
- IRB interface shows incorrect bandwidth value. [PR1302202](#)
- AFEB might not come up if LFM is deactivated. [PR1306707](#)
- After executing the **request system reboot both** CLI command, the PPP daemon might become unresponsive. [PR1310909](#)
- The PPPoE subscriber might not be able to login correctly after it fails to authenticate in a subscriber scenario. [PR1311113](#)
- The jpppd process might generate a core file at telemetry_start_timer, mosquito_handle_connack, and telemetry_mqtt_publisher. [PR1311396](#)
- The ifinfo process might crash and generate a core file when you execute the CLI command **show interfaces <Name>** command with the name greater than 128 characters. [PR1313827](#)
- Benign error messages are seen during an unified ISSU of MX Series Virtual Chassis if unsupported FRUs are present. [PR1316374](#)
- There is no route to IP address from the directly connected route on the static VLAN DEMUX interface. [PR1318282](#)
- **IPv6 Framed Interface Id** field (from **show subscribers extensive** output) does not match the negotiated value. [PR1321392](#)
- Interfaces might not work properly after FPC restarts. [PR1329896](#)
- The transportd process might crash when there is an SNMP query on jnxoptIfOChSinkCurrentExtTable with unsupported interface index. [PR1335438](#)
- Traffic loss might be seen after deleting aggregated Ethernet bundle unit 1. [PR1329294](#)

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](#)
- PPPoE or DHCP clients cannot log in to PPPoE or DHCP dual-stack subscriber scenario. [PR1298976](#)
- Multiple jdhcpd core files are observed in jdhcpd_update_groups at `../..../src/junos/usr/sbin/jdhcpd/jdhcpd_config.c:2290`. [PR1311569](#)
- DHCPv6 traffic might be dropped in a subscriber scenario. [PR1316274](#)
- The jdhcpd process might generate a core file after making DHCP configuration changes. [PR1324800](#)
- The **on-demand-address-allocation** option of the **dual-stack-group** statement does not work for IPv6. [PR1327681](#)
- The jdhcpd process crashes and generates a core file. [PR1334230](#)

MPLS

- Minor difference is seen between mpls.statistics and the adjusted bandwidth. [PR1259500](#)
- An ingress RSVP LSP fails to come up when the **clear rsvp lsp** command is run on the egress router. [PR1275563](#)
- The rpd might crash in LDP L2 circuit scenario. [PR1275766](#)
- The traffic is dropped during NSR switchover for RSVP P2MP provider tunnels are used by MVPN. [PR1293014](#)
- The traffic in P2MP tunnels might be lost when the next-generation MVPN uses RSVP-TE. [PR1299580](#)
- The rpd process might crash in rare scenarios where traffic engineering is configured. [PR1303239](#)
- kysncd process might crash after the backup Routing Engine is removed/uninstalled and then reinserted/reinstalled, [PR1303491](#)
- BGP multipath might not work if the interface flaps. [PR1305228](#)
- The configuration of the **explicit-null** statement might block host-bound traffic incoming from LSP. [PR1305523](#)
- RSVP node-hello works incorrectly after the next hop for the remote destination is changed. [PR1306930](#)
- On a router with UHP-based LSP configuration, the rpd process might crash when interfaces are down. [PR1309397](#)
- The rpd process might crash when LDP updates the label for BGP route. [PR1312117](#)
- The rpd might crash when LDP sessions and RSVP LSPs are flapped in an LDP over RSVP setup. [PR1318480](#)
- The IPv4 or 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 interfaces across Virtual Chassis members. [PR1320742](#)

- The rpd crashes with **ldp p2mp** configuration. [PR1321626](#)
- The rpd process crashes and generates a core file in jemalloc_block_mallocx because of a memory leak. [PR1321952](#)
- SNMP OID counters for mplsLspInfoAggrOctets might show a constant value for RSVP LSPs for longer time in case of route withdrawn scenario. [PR1327350](#)
- Local repair took about 150 milliseconds greater than expected 100 milliseconds. [PR1327988](#)
- Packet loss might be observed when auto-bandwidth for CCC connections is enabled. [PR1328129](#)
- The rpd process crashes on backup Routing Engine because of memory exhaustion. [PR1328974](#)

Network Management and Monitoring

- On MX Series platform, the Routing Engine does not reply to SNMP request. [PR1240178](#)
- When the SNMP configuration gets activated, the snmpd process starts to consume a lot of CPU time. [PR1300016](#)
- The syslog might generate duplicate entries of hostname and timestamp. [PR1304160](#)
- The mib2d process generates a core file when an FPC is reset during asynchronous statistic collection through SNMP. [PR1318302](#)
- With **interface-mib** configuration in a dynamic-profile, when multiple OIDs are queried in a SNMPGET and SNMPWALK, the router might reply with **No Such Instance currently exists at this OID** for some of the OIDs. [PR1329749](#)

Platform and Infrastructure

- Adaptive load balancing (ALB) functionality is supported only for unicast traffic. If the aggregate bundle contains logical interfaces for a bridge or VPLS domains, flooded traffic might be dropped. [PR821237](#)
- The Packet Forwarding Engine on an MS-MPC might crash with a large scale routes for MX Series routers. [PR1277264](#)
- The FPC **resource-monitor % mem free** values for next-hop forwarding are incorrect. [PR1287592](#)
- There might be Packet Forwarding Engine memory leak when the next-hop address that is defined in the next-hop group is reachable through multiple interfaces. [PR1287870](#)
- Dynamic MAC learning might fail on GRE tunnel interfaces. [PR1291015](#)
- RMOPD_HW_TIMESTAMP_INVALID is reported two to four times a day, which raises an alarm when polled through the jnxRpmResSumPercentLost MIB. [PR1300049](#)
- Traffic getting dropped in egress Packet Forwarding Engine because of hashing mismatch. [PR1300789](#)
- Packet Forwarding Engine might crash after the MPC is reset in a firewall filter scenario. [PR1300990](#)
- Classifiers do not get applied on the aggregated Ethernet member links when CoS is configured on MX Series routers with DPCs. [PR1301723](#)

- MX Series MPC wedges (might cause fabric blackhole and finally reboot the line card) when creating more than 4000 logical tunnel interfaces per Packet Forwarding Engine. [PR1302075](#)
- The **interface-mac-limit** configuration might fail for aggregated Ethernet interfaces. [PR1303293](#)
- The TWAMP Request-TW-Session message's Type-P Descriptor format is not RFC-compliant. [PR1305752](#)
- On MX Series routers with MPCs or MICs, the resource monitor (RSMON) thread might be stuck in a loop consuming 100 percent of FPC line card CPU. [PR1305994](#)
- System reach process ceiling <low> watermark due to auditd. [PR1305964](#)
- The source MACs might be leaked or not learned between different VPLS instances at the received VPLS PE devices. [PR1306293](#)
- The RPM probe with probe interval of 1 second fails in MX Series routers. [PR1308952](#)
- The expected error message is not observed during a Telnet session when a username longer than acceptable limit is used. [PR1312265](#)
- ICMP error messages are observed in the Packet Forwarding Engine. [PR1313668](#)
- Rate-limit configured with small temporal buffer size might cause packet loss. . [PR1317385](#)
- Multicast traffic is not forwarded on the newly added P2MP branch or receiver. [PR1317542](#)
- Multicast traffic might get duplicated when MoFRR is configured. [PR1318129](#)
- The GNF-associated MPC hangs during reboot after a unified ISSU. [PR1318394](#)
- Change in default severity of correctable ECC errors on MX Series routers from fatal to major. [PR1320585](#)
- Errors might be observed when **fabric-header-crc-enable** feature is enabled. [PR1320874](#)
- The rate limit with a lock protected variable of netisr queue, the count of packets in netisr queue becomes wrong. This leads to kernel crash or debugger command prompt. [PR1332153](#)
- RPM probes delegated to MS-MIC get stuck when any change is made on BGP group configuration. [PR1322097](#)
- The **no-propagate-ttl** configuration might not take effect when **chained-composite-next-hop ingress l3vpn extended-space** is configured. [PR1323160](#)
- MX Series Virtual Chassis MAC learning does not occur on specific interfaces. [PR1327723](#)
- The packet might get dropped in LSR when MPLS pseudowire payload does not have a control word and the packet's destination MAC address starts with 4 or 6. [PR1327724](#)
- Traffic loss might be observed on a logical tunnel interface. [PR1328371](#)
- Junos OS automation folder lost execution permissions. [PR1328570](#)
- SNMP pingResultsMinRtt, pingResultsMaxRtt, pingResultsAverageRtt and pingProbeHistoryResponse are marked as "1" instead of "0" if the response is not received from the RPM server. [PR1333320](#)

- Traffic loss might be seen for some flows because of the churn in the network. [PR1335302](#)
- Route corruption in Packet Forwarding Engine with connectivity-fault-management enabled for Layer 2 circuit. [PR1338854](#)

Routing Policy and Firewall Filters

- The rpd process might crash when **vrf-target auto** is configured for a routing instance. [PR1301721](#)
- The policy configuration might not be evaluated if policy expression is changed. [PR1317132](#)

Routing Protocols

- The command **show bgp summary** results incorrect while assisting a graceful restart. [PR1045151](#)
- BGP MIBv2 enterprise MIB objects for InetAddress types are not properly generating OIDs. [PR1265504](#)
- The rpd process might crash when BGP is deactivated or activated. [PR1272202](#)
- When the bfdd process restarts, an issue with next-generation MVPN and L2VPN route exchange causes MVPN and VPLS traffic to be dropped. [PR1278153](#)
- BGP updates might not be advertised to peers completely in certain conditions. [PR1282531](#)
- Some BGP-related traceoptions flag settings are not effective immediately when the configuration is committed, until the BGP sessions are flapped. [PR1285890](#)
- In IS-IS service request (SR) LAN scenario, advertising adjacencysegment identifiers might be missed for a few neighbors if the TLV length gets exhausted. This is not a common scenario. [PR1288331](#)
- Multihop BFD sessions flap continuously. [PR1291340](#)
- The link management protocol daemon (lmpd) repeatedly crash when a logical system is configured on the same router. [PR1294166](#)
- The rpd process might crash because of the AS PATH check error when RIB groups are added first and the routing instance later. [PR1298262](#)
- MSDP sessions might flap because data replication might get stuck between backup and master Routing Engine with a huge SA burst between peers. [PR1298609](#)
- When the device is restarted with Junos OS Release 17.4R1, the benign error message **channel 0: chan_shutdown_read: shutdown() failed for fd 10 [i0 o3]: Socket is not connected** messages may show up with no functionality impact are seen. [PR1300409](#)
- IBGP route damping does not take effect on VPN address families. [PR1301519](#)
- The rpd process might crash, generating a core file, when a multipath route is deleted. [PR1302395](#)
- The mcsnoopd process generates a core file at __raise, abort, __task_quit__, task_quit, task_terminate_timer_callback, task_timer_dispatch, and task_scheduler_internal (enable_slip_detector=true, no_exit=true) at `../src/junos/lib/libjtask/base/task_scheduler.c:275`. [PR1305239](#)

- The BFD session might flap when querying interface statistics through SNMP or CLI show command in vMX. [PR1305308](#)
- 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](#)
- Qualified next-hop resolution fails in some scenarios when there is a next-hop interface specified. [PR1308800](#)
- BGP labeled unicast protection might break multicast reverse path forwarding (RPF). [PR1310036](#)
- When NSR is configured, the BGP session might flap if the connection between the master Routing Engine and the backup Routing Engine keeps flapping. [PR1311224](#)
- The rpd process might crash and generate a core file in **bgp_rt_send_message at ../../../../src/junos/usr/sbin/rpd/bgp/bgp_io.c:1460** . [PR1310751](#)
- Dedicated BFD does not work on MX Series platforms. [PR1312298](#)
- IS-IS SPF gets triggered by LSP updates containing changes in reservable bandwidth in TE extensions. [PR1313147](#)
- The routing protocol process (rpd) might crash and generate a core file. [PR1314679](#)
- BGP prefixes with three levels of recursion for resolution gets stuck with a stale next hop at the first level after a link-down event. [PR1314882](#)
- The SUB-TLV values are assigned for segment routing TE policy SUB-TLVs. [PR1315486](#)
- On a router with BGP Monitoring Protocol (BMP) configured, the rpd process might crash when the rpd process is gracefully terminated. [PR1315798](#)
- The link-state database (LSDB) entry cleanup might cause the rpd process to crash, if loop-free alternate is configured. [PR1317023](#)
- When two Route-reflector (RR) routers use PIC (protect core) to protect each other's BGP-LU (labeled-unicast) LSP, endless label oscillation might be seen. [PR1318093](#)
- The routing protocol process (rpd) crash is seen when deactivating static route if the next-hop interface is point-to-point (P2P) type. [PR1323601](#)
- Multiple next hops might not be installed for IBGP multipath route after IGP route updates. [PR1327904](#)
- With BGP, LDP, and IS-IS configurations, deleted IS-IS routes might still be visible in the RIB. [PR1329013](#)
- The rpd might crash on backup Routing Engine after BGP peer is deleted. [PR1329932](#)
- When prefix limit is reached, increasing maximum-prefixes does not take effect immediately. [PR1323765](#)
- BGP session get stuck in active state after remote end router is upgraded. [PR1335319](#)
- When the primary interface is back online, the discarded next hop address is retained until the BGP LU neighbor is cleared. This impacts the cloned route (S=0) only. [PR1333570](#)

Services Applications

- When configuring a NAT pool that is shared between PCP and standard NAT, the PCP mappings cannot be cleared. [PR1284261](#)
- The jl2tpd process might stop responding shortly after GRES. [PR1295248](#)
- L2TP subscribers might get stuck in a terminating state during login. [PR1298175](#)
- L2TP tunnel switch clients experience packets drops for large packets because of fragmentation in a L2TP tunnel switch. [PR1312691](#)
- When an l2tp subscriber BNG receives ANCP port up with TLV DSL-type=0 ("other"), the BNG does not include AVP 145 in the ICRQ packet. [PR1313093](#)
- L2TP tunnel Tx and Rx bytes count sometimes decrease when subscriber sessions are reduced within the tunnel. [PR1318133](#)
- In an L2TP scenario, the MRU might be changed to 1492 instead of the default 1500. [PR1319252](#)
- IPCP active mode remains disabled for MLPPP on LNS. [PR1319580](#)
- Stale L2TP routes might be seen when L2TP peer uses any UDP port other than the default. [PR1322197](#)
- L2TP tunnel switch might drop the first **CHAP Success** packet from LNS because of the delay in programming of the /136 route on the Packet Forwarding Engine. [PR1325528](#)
- In case the number of sessions addressed in CSURQ is more than about 107, not all CSURQ messages receive a response. [PR1330150](#)

Subscriber Access Management

- Service interim for DHCP subscribers does not work in a JSRC scenario. [PR1303553](#)
- The **show network-access aaa accounting** command might display additional entries. [PR1304594](#)
- Incorrect **Acct-Delay-Time** in RADIUS **Accounting-On** message is seen after the MX Series router, acting as a BNG, is rebooted. [PR1308966](#)
- Service interim for random users is missing in a JSRC scenario. [PR1315207](#)
- The delegated prefix from RADIUS is incorrectly parsed when the prefix is fewer than 20 bytes long. [PR1315557](#)
- The PPPoE subscribers might encounter connection failure during login. [PR1317019](#)
- The unified ISSU is allowed to proceed when the account is suspended. [PR1320038](#)
- Incorrect address assignment sequence is seen from linked IP pools. [PR1323829](#)
- The general authentication service considers the RADIUS attributes Framed-IPv6-Prefix = ::/64 and Delegated-IPv6-Prefix = ::/56 as valid parameters. [PR1325576](#)
- The MX204 does not send the RADIUS Accounting-Off message. [PR1327822](#)
- Subscriber management experiences SDB DOWN event; dfcd[4707]: %DAEMON-3: attempting to close SDB while DOWN. [PR1336388](#)

User Interface and Configuration

- The commit time increases every time. [PR1029477](#)
- The CLI session might be terminated while the **show configuration | compare rollback 1** command is issued. [PR1331716](#)

VPNs

- 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 **LD** (local site signaled down) state. [PR1305873](#)
- A nonoptimal route to source might be selected for next-generation MVPN with **unicast-umh-election** enabled. [PR1315011](#)
- Un-hide the **set protocols pim mvpn family inet6 disable** configuration to allow the users to disable the inet6 configuration on MVPN. [PR1317767](#)
- The routing protocol process (rpd) might stop responding after a unified ISSU in a large-scale scenario with PIM configuration. [PR1322530](#)
- Moving MC-LAG from LDP-based pseudowire to BGP-based pseudowire might cause an rpd crash. [PR1325867](#)
- In an next-generation MVPN and NSR configuration, the rpd process might crash and generate a core file on the backup Routing Engine. [PR1328246](#)

SEE ALSO

[New and Changed Features | 90](#)

[Changes in Behavior and Syntax | 110](#)

[Known Behavior | 115](#)

[Known Issues | 119](#)

[Documentation Updates | 154](#)

[Migration, Upgrade, and Downgrade Instructions | 155](#)

[Product Compatibility | 162](#)

Documentation Updates

IN THIS SECTION

- [New Simplified Documentation Architecture | 154](#)

This section lists the errata and changes in Junos OS Release 18.1R2 documentation for MX Series.

New Simplified Documentation Architecture

- With the release of Junos OS Release 18.1, Juniper is simplifying its technical documentation to make it easier for you to find information and know that you can rely on it when you find it. In the past, we organized documentation about Junos OS software features into platform-specific documents. In many cases, features are supported on multiple platforms, so you might not easily find the document you want for your platform.

With Junos OS Release 18.1, we have eliminated the platform-specific software feature documents. For example, if you want to find documentation on OSPF, there is only one document regardless of which platform you have. Here are some of the benefits of our new simplified architecture:

- Over time, you will see better search results when looking for Juniper documentation. You will be able to find what you want faster and be assured that is the right document.
- If a software feature is supported on multiple platforms, you can find information about all the platforms in one place.
- Because we have eliminated many documents that covered similar topics, you will now find one document with all the information.
- You can know that you are always getting the most current and accurate information.

SEE ALSO

[New and Changed Features | 90](#)

[Changes in Behavior and Syntax | 110](#)

[Known Behavior | 115](#)

[Known Issues | 119](#)

[Resolved Issues | 128](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading to Release 18.1 | 156](#)
- [Procedure to Upgrade to FreeBSD 11.x based Junos OS | 156](#)
- [Procedure to Upgrade to FreeBSD 6.x based Junos OS | 158](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 160](#)
- [Upgrading a Router with Redundant Routing Engines | 161](#)
- [Downgrading from Release 18.1 | 161](#)

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

Starting in Junos OS 18.1R1 release, FreeBSD 11.x is the underlying OS for all Junos OS platforms which were previously running on FreeBSD 10.x based Junos OS. FreeBSD 11.x does not introduce any new Junos OS related modifications or features but is the latest version of FreeBSD.

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

Platform	FreeBSD 6.x-based Junos OS	FreeBSD 11.x-based Junos OS
MX5, MX10, MX40, MX80, MX104	YES	NO
MX204, MX240, MX480, MX960, MX2010, MX2020 MX10003, vMX	NO	YES

Basic Procedure for Upgrading to Release 18.1

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 11.x based Junos OS

Platforms impacted: MX204, MX240, MX480, MX960, MX2010, MX2020, MX10003, and vMX.

To download and install FreeBSD 11.x based Junos OS:

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/>
2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.
4. Select the **Software** tab.
5. In the **Install Package** section of the **Software** tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.

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

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

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-32-18.1R2.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-64-18.1R2.9-signed.tgz
```

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-32-18.1R2.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-64-18.1R2.9-limited.tgz
```

Replace **source** with one of the following values:

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

- `http://hostname/pathname`
- `scp://hostname/pathname`

Do not use the **validate** option while upgrading from Junos OS (FreeBSD 6.x) to Junos OS (FreeBSD 11.x). This is because programs in the **junos-upgrade-x** package are built based on FreeBSD 11.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 the VM Host Installation topic in the [Installation and Upgrade Guide](#).

NOTE: After you install a Junos OS Release 18.1 **jinstall** package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add no-validate** command and specify the **jinstall** package that corresponds to the previously installed software.

NOTE: Most of the existing **request system** commands are not supported on routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. See the VM Host Software Administrative Commands in the [Installation and Upgrade Guide](#).

Procedure to Upgrade to FreeBSD 6.x based Junos OS

Platforms impacted: MX5, MX10, MX40, MX80, MX104.

To download and install FreeBSD 6.x based Junos OS:

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/>
2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.
4. Select the **Software** tab.
5. In the **Install Package** section of the **Software** tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **jinstall** package on the routing platform.

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

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

```
user@host> request system software add validate reboot source/jinstall-ppc-18.1R2.9-signed.tgz
```

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

```
user@host> request system software add validate reboot  
source/jinstall-ppc-18.1R2.9-limited-signed.tgz
```

Replace **source** with one of the following values:

- **/pathname**—For a software package that is installed from a local directory on the router.

- For software packages that are downloaded and installed from a remote location:

- `ftp://hostname/pathname`
- `http://hostname/pathname`
- `scp://hostname/pathname`

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 18.1 **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 17.1, 17.2 and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

Upgrading a Router with Redundant Routing Engines


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

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

For the detailed procedure, see the [Installation and Upgrade Guide](#).

Downgrading from Release 18.1

To downgrade from Release 18.1 to another supported release, follow the procedure for upgrading, but replace the 18.1 jinstall package with one that corresponds to the appropriate release.


NOTE: You cannot downgrade more than three releases.

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

SEE ALSO

New and Changed Features 90
Changes in Behavior and Syntax 110
Known Behavior 115
Known Issues 119
Resolved Issues 128
Documentation Updates 154
Product Compatibility 162

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 162](#)

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 | 90](#)

[Changes in Behavior and Syntax | 110](#)

[Known Behavior | 115](#)

[Known Issues | 119](#)

[Resolved Issues | 128](#)

[Documentation Updates | 154](#)

[Migration, Upgrade, and Downgrade Instructions | 155](#)

Junos OS Release Notes for NFX Series

IN THIS SECTION

- New and Changed Features | 163
- Changes in Behavior and Syntax | 167
- Known Behavior | 168
- Known Issues | 170
- Resolved Issues | 173
- Documentation Updates | 175
- Migration, Upgrade, and Downgrade Instructions | 176
- Product Compatibility | 179

These release notes accompany Junos OS Release 18.1R2 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/software/junos/>

New and Changed Features

IN THIS SECTION

- Release 18.1R2 New and Changed Features | 164
- Release 18.1R1 New and Changed Features | 164

This section describes the new features or enhancements to existing features in Junos OS Release 18.1R2 for NFX Series devices.

Release 18.1R2 New and Changed Features

There are no new features or enhancements to existing features for NFX Series in Junos OS Release 18.1R2.

Release 18.1R1 New and Changed Features

Hardware

- **NFX150 platform**—Starting with Junos OS Release 18.1R1, the NFX150 Network Services Platform is available as a single platform that integrates routing, switching, and security functions. The NFX150 is a secure, automated, software-driven customer premises equipment (CPE) platform that delivers virtualized network and security services on demand. It is suited for small to medium-sized enterprises and acts as a secure router, SD-WAN CPE, or uCPE. The architecture of the NFX150 platform enables unified management of all its components through the Junos Control Plane (JCP). It also offers effective management of the system resources and reduced system boot time.

The NFX150 portfolio is available in the following variants:

- **NFX150-S1**—Rack-mount model with 2.2-GHz 8-core Intel CPU, 200-GB SSD, 16-GB RAM, four 10/100/1000BASE-T RJ-45 LAN ports, and two 1-Gigabit Ethernet/10-Gigabit Ethernet SFP+ WAN ports.
- **NFX150-S1E**—Rack-mount model with 2.2-GHz 8-core Intel CPU, 200-GB SSD, 32-GB RAM, four 10/100/1000BASE-T RJ-45 LAN ports, and two 1-Gigabit Ethernet/10-Gigabit Ethernet SFP+ WAN ports.

NFX150-S1 and NFX150-S1E support the following expansion modules:

- **NFX-EM-6T2SFP**—Expansion module with six 1-Gigabit Ethernet RJ-45 ports and two 1-Gigabit Ethernet SFP ports
- **NFX-LTE-AE**—Expansion module with an LTE modem supporting the frequency bands in Europe and North America.
- **NFX-LTE-AA**—Expansion module with an LTE modem supporting the frequency bands in Asia and Australia.
- **NFX150-C-S1**—Compact desktop model with 2.2-GHz 4-core Intel CPU, 8-GB RAM, 100-GB SSD, four 10/100/1000BASE-T RJ-45 LAN ports, and two 1-Gigabit Ethernet/10-Gigabit Ethernet SFP+ WAN ports.
- **NFX150-C-S1-AE**—Compact desktop model with 2.2-GHz 4-core Intel CPU, 8-GB RAM, 100-GB SSD, four 10/100/1000BASE-T RJ-45 LAN ports, and two 1-Gigabit Ethernet/10-Gigabit Ethernet SFP+ WAN ports. This device provides integrated LTE modem for Europe and North America.
- **NFX150-C-S1-AA**—Compact desktop model with 2.2-GHz 4-core Intel CPU, 8-GB RAM, 100-GB SSD, four 10/100/1000BASE-T RJ-45 LAN ports, and two 1-Gigabit Ethernet/10-Gigabit Ethernet SFP+ WAN ports. This device provides integrated LTE modem for Asia, Australia, and New Zealand.

- NFX150-C-S1E-AE—Compact desktop model with 2.2-GHz 4-core Intel CPU, 16-GB RAM, 100-GB SSD, four 10/100/1000BASE-T RJ-45 LAN ports, and two 1-Gigabit Ethernet/10-Gigabit Ethernet SFP+ WAN ports. This device provides integrated LTE modem for Europe and North America.
- NFX150-C-S1E-AA—Compact desktop model with 2.2-GHz 4-core Intel CPU, 16 GB RAM, 100 GB SSD, four 10/100/1000BASE-T RJ-45 LAN ports, and two 1-Gigabit Ethernet/10-Gigabit Ethernet SFP+ WAN ports. This device provides integrated LTE modem for Asia, Australia, and New Zealand.
- **Transceivers** –NFX150 supports the following optics:
 - 10-gigabit SFP+ transceivers: EX-SFP-10GE-USR, EX-SFP-10GE-SR, EX-SFP-10GE-LR, EX-SFP-10GE-ER, EX-SFP-10GE-DAC-1M, EX-SFP-10GE-DAC-3M, EX-SFP-10GE-DAC-5M, EX-SFP-10GE-DAC-7M
 - 1-gigabit SFP transceivers: EX-SFP-1GE-SX, EX-SFP-1GE-SX-ET, EX-SFP-1GE-LX, EX-SFP-1GE-LH, EX-SFP-1GE-LX40K, EX-SFP-GE80KCW1470, EX-SFP-GE80KCW1490, EX-SFP-GE80KCW1510, EX-SFP-GE80KCW1530, EX-SFP-GE80KCW1550, EX-SFP-GE80KCW1570, EX-SFP-GE80KCW1590, EX-SFP-GE80KCW1610

NOTE: USR and ER optics are displayed as SFP+-10G-ER in the **show system inventory hardware optics** command output.

Amphenol DAC 1M and 3M cables are displayed as **unknown** in the **show system inventory hardware optics** command output.

[See [NFX150 Network Services Platform Hardware Guide](#).]

Service Chaining

- **VNF service chaining**—Starting with Junos OS Release 18.1R1, the NFX150 device supports deploying and service chaining of multiple, secure, high-performance virtualized network functions (VNFs) as a single device. The Junos Control Plane (JCP) runs on the Junos VM and functions as the single point of management for the chassis and VNFs.

[See [Service Chaining on NFX Devices](#).]

Security

- **Secure Boot**—Starting with Junos OS Release 18.1R1, the NFX150 devices support secure boot implementation, which is based on the UEFI 2.4 standard. The BIOS has been hardened and serves as a core root of trust. The BIOS updates, bootloader, and kernel are cryptographically protected. No action is required to implement secure boot.

[See [Feature Explorer](#) and enter Secure Boot.]

Layer 2 Features and Protocols

- **Layer 2 features**—Starting with Junos OS Release 18.1R1, the NFX150 supports Layer 2 features such as VLANs, IGMP snooping, MLDv1 snooping, MLDv2 snooping, port mirroring, port security, and the Link Layer Discovery Protocol (LLDP).

[See [Services](#) and [Ethernet Switching](#).]

Layer 3 Features and Protocols

- **Layer 3 features**—Starting with Junos OS Release 18.1R1, the NFX150 supports Layer 3 features such as IP Security (IPsec), firewall filters, port mirroring, BFD, and class of service (CoS). It also supports Layer 3 protocols such as BGP, RIP, OSPFv1, OSPFv2, and IS-IS.

[See [IPsec](#) and [Security](#).]

Fault Management

- **OAM link fault management and connectivity fault management**—Starting with Junos OS Release 18.1R1, NFX150 devices support configuration of IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters. The IEEE 802.3ah standard meets the requirement for OAM capabilities even as Ethernet moves from being solely an enterprise technology to a WAN and access technology, and the standard remains backward-compatible with existing Ethernet technology.

The IEEE 802.1ag specification provides for Ethernet connectivity fault management (CFM). CFM monitors Ethernet networks that might comprise one or more service instances for network-compromising connectivity faults.

[See [Fault Management](#).]

Network Service Orchestrator

- **Network Service Orchestrator**—Starting with Junos OS Release 18.1R1, NFX150 devices support Network Service Orchestrator, which is a client included in the base software of the NFX150 device, and connects to the Network Activator deployed on a cloud or server. The Network Activator application intelligently automates service life cycle management of managed VPN networks, in-region secured Internet connections, and out-of-region IPsec connections on NFX150 devices. This application enables the booting and configuration of the NFX150 device when it is first powered on.

[See [Network Activator Overview](#).]

Wireless WAN

- **Wireless WAN**— Starting with Junos OS Release 18.1R1, the following NFX150 device models provide wireless WAN support through the LTE module:
 - NFX150-S1
 - NFX150-S1E
 - NFX150-C-S1-AE
 - NFX150-C-S1-AA
 - NFX150-C-S1E-AE
 - NFX150-C-S1E-AA

[See [NFX150 Network Services Platform Hardware Guide](#).]

SEE ALSO

Changes in Behavior and Syntax 167
Known Behavior 168
Known Issues 170
Resolved Issues 173
Documentation Updates 175
Product Compatibility 179

Changes in Behavior and Syntax

IN THIS SECTION

- [CLI | 168](#)

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 18.1R2 for the NFX Series.

CLI

- Starting with Junos OS Release 18.1R1, the host-os hierarchy level is replaced with the vmhost hierarchy level for NFX150 devices.

SEE ALSO

New and Changed Features 163
Known Behavior 168
Known Issues 170
Resolved Issues 173
Documentation Updates 175
Product Compatibility 179

Known Behavior

IN THIS SECTION

- [Known Behavior: 18.1R2 | 169](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.1R2 for the NFX Series.

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

Known Behavior: 18.1R2

- The file transfer rate from an external media over the network to an NFX150 device is around 40–50 Mbps.

[PR1290263](#)

- On NFX150 devices running Junos OS Release 18.1, service chaining can be achieved through front panel ports by using SR-IOV. For the switching to work through SR-IOV enabled front panel port, the physical NIC port must be up and operational.

[PR1319294](#)

- On NFX150 devices running Junos OS Release 18.1, you cannot use the **request system software scripts** command to add script packages on the Junos OS.

[PR1333061](#)

- On NFX150 devices running Junos OS Release 18.1, traffic shaping on tunnel interfaces such as IP-IP and GRE is not supported.

[PR1335582](#)

- On NFX150 devices running Junos OS Release 18.1, Transcend does not support Linux based SSD firmware upgrade mechanism in field for its SSD. Hence, field upgrade of Transcend SSD firmware cannot be provided for NFX150 devices.

[PR1347562](#)

SEE ALSO

[New and Changed Features | 163](#)

[Changes in Behavior and Syntax | 167](#)

[Known Issues | 170](#)

[Resolved Issues | 173](#)

[Documentation Updates | 175](#)

[Product Compatibility | 179](#)

Known Issues

IN THIS SECTION

- [Known Issues: 18.1R2 | 170](#)

This section lists the known issues in hardware and software in Junos OS Release 18.1R2 for the NFX Series.

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

Known Issues: 18.1R2

- On NFX150 devices, you cannot generate an ISO configuration image. [PR1316900](#)
- On NFX150 devices, connectivity fault management (CFM) is not supported on circuit cross-connect (CCC) interfaces. [PR1311588](#)
- There is no commit check if the PCI address is reused for different interfaces in a VNF. As a workaround, we recommend that you stop the VNF and then add or delete interfaces. [PR1205497](#)
- The **show chassis routing-engine** command displays the last reboot reason as **power cycle/failure** even for a normal system reboot. In addition, the logs record an abnormal shutdown message. [PR1232501](#)
- Configuring more than the available number of virtual functions for an SR-IOV front panel port, might result in a state where the user MAC addresses for such interfaces are not released back to the System MAC Pool on deletion of the VNF. [PR1259975](#)
- On NFX150 devices with LTE support running Junos OS Release 18.1, the **show system visibility cpu** command does not display CPU pinning information for LTE. There is no known workaround. [PR1347609](#)
- While changing port mapping configuration across FPC0 and FPC1 on NFX150 devices with expansion module, forwarding path simulation process for FPC0 may crash when FPC0 restarts for port mapping configuration to take effect. This results in an additional reboot of FPC0. After the reboot, FPC0 recovers automatically and appears online. [PR1347259](#)
- LTE functions as a kernel driver for modem packet handling and should not be treated as a customized VNF. The **request** command does not provide console support. [PR1348196](#)
- On NFX150 devices running Junos OS Release 18.1, manually loading the factory-default configuration on the device might not set up the necessary configurations for Remote Activation to work. As a workaround, before loading the factory default configuration on the device, ensure that the configuration for phone-home is deleted and committed. [PR1347308](#)

- On NFX150 devices running Junos OS Release 18.1, Dev key revocation is not supported by BIOS. Dev key revocation is to prevent customers from installing Dev signed image by mistake on their setup. [PR1344738](#)
- On NFX150 devices running Junos OS Release 18.1, enabling hugepages for VNFs and pre-reserving of hugepages are not supported. Hence, the following commands are not supported:
 - **set system memory hugepages**
 - **set virtual-network-functions vnf-name memory features hugepages**[PR1360998](#)
- On NFX150 devices running Junos OS Release 18.1, traffic statistics for 10-Gigabit Ethernet host interfaces are not displayed correctly. [PR1348720](#)
- On NFX150 devices running Junos OS Release 18.1, syslog messages do not display xauth client authentication information such as assigned IP address and DNS. [PR1305078](#)
- On NFX150 devices running Junos OS Release 18.1, FTP displays an error message, **ftpd[14105]: bl_init: connect failed for `/var/run/blacklistd.sock' (No such file or directory.** [PR1315605](#)
- On NFX150 devices running Junos OS Release 18.1, CLI output for the **show security ipsec inactive-tunnels** command is incomplete. [PR1325763](#)
- On NFX150 devices running Junos OS Release 18.1, error messages are seen while rebooting the FPC0 interface. [PR1326487](#)
- On NFX150 devices running Junos OS Release 18.1, commit is successful with any message on the console while creating a VNF using CLI. However, VNF may not be created due to some errors. Syslog will show error messages with reasons for not creating the VNF. [PR1333057](#)
- On NFX150 devices running Junos OS Release 18.1, **file put** operation by a user with no super-user permissions might fail. [PR1333991](#)
- On NFX150 devices running Junos OS Release 18.1, **file copy** operation by a user with no super-user permissions might fail. [PR1333995](#)
- On NFX150 devices running Junos OS Release 18.1, extracting contents of an archived file by using the **tar -xzf** command might fail.

[PR1334485](#)

- On NFX150 devices running Junos OS Release 18.1, the **op** command, which is used to execute python scripts that are residing on the JCP might fail and result in an error. As a workaround, delete the configuration knob **system scripts op allow-url-for-python** and re-run the **op** command by using CLI.

[PR1360806](#)

- During BIOS upgrade process, it does not display the existing BIOS version or the new BIOS version to which it is being upgraded. Similarly, it does not display the BIOS version when a lower version of BIOS is getting upgraded to a higher version of BIOS.

[PR1342573](#)

- On NFX150 devices running Junos OS Release 18.1, the LTE interface may not work with Vodafone-India sim.

[PR1343741](#)

- On NFX150 devices running Junos OS Release 18.1, after upgrading the image, the SYSHMD error messages are observed only once.

[PR1341005](#)

- On NFX150 devices running Junos OS Release 18.1, after upgrading the image, FPC0, FPC1 IFL error messages are observed only once.

[PR1341583](#)

- On NFX150 devices running Junos OS Release 18.1, **request ca-certificate** command fails. CA Trust certificates cannot be installed on the device.

[PR1343474](#)

- On NFX150 devices running Junos OS Release 18.1, the MTU of an heth interface cannot be set. The configuration knob of **set vmhost interfaces heth-X-Y mtu** is not supported.

[PR1346876](#)

- On the NFX150 running Junos OS Release 18.1, the rssi value for Wireless Model interface cl-1/1/0 shows negative value.

[PR1344377](#)

SEE ALSO

[New and Changed Features | 163](#)

[Changes in Behavior and Syntax | 167](#)

[Known Behavior | 168](#)

[Resolved Issues | 173](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 18.1R2 | 173](#)
- [Resolved Issues: 18.1R1 | 174](#)

This section lists the issues fixed in the Junos OS main release and the maintenance releases for NFX Series devices.

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

Resolved Issues: 18.1R2

Junos Control Plane (NFX150)

- Under some circumstances, FPC0 ukern of NFX150 may crash and restart. The FPC recovers automatically and it does not crash again after the recovery. There is no known workaround. [PR1347629](#)
- On NFX150 devices running Junos OS Release 18.1, jdmd core is observed after configuration changes failed to commit.

[PR1348783](#)

- On NFX150 devices running Junos OS Release 18.1, while changing port mapping configuration on FPC0 and FPC1 interfaces by using expansion module, memory corruption is detected in low memory and DMA Write errors are observed.

[PR1325585](#)

- On NFX150 devices running Junos OS Release 18.1, there could be a core related to Key Management Daemon (kmd) during some configuration changes. The issue is very rare.

[PR1330280](#)

- On NFX150 devices running Junos OS Release 18.1, vm core is observed while downloading the image from PHS.

[PR1330487](#)

- On NFX150 devices running Junos OS Release 18.1, mac-table entries are not updated with topology change notification (TCN).

[PR1326593](#)

- On NFX150 devices running Junos OS Release 18.1, with default LTE configuration, the PHC on the device will not be able to communicate with Juniper redirect server with LTE as the only link on the device. The name resolution of Juniper redirect server will fail without fixing this issue.

[PR1342499](#)*Juniper Device Manager (NFX250)*

- On NFX250 devices running Junos OS Release 18.1, if the same VLAN ID is used in two different cross-connect configurations, the commit will not fail.

[PR1346698](#)**Resolved Issues: 18.1R1***Juniper Device Manager (NFX250)*

- If a VNF requests for more memory than the available system memory, commit might go through without any errors resulting in VNF going into a shut off state. As a workaround, use the show system visibility memory command to check the available free memory before spawning a VNF. Alternatively, check the log files and the VNF shut off reason will be captured in /var/log/syslog file. [PR1221647](#)
- While spawning a VNF, there might not be a commit check for the valid image type supported. [PR1221642](#)

SEE ALSO

New and Changed Features 163
Changes in Behavior and Syntax 167
Known Behavior 168
Known Issues 170
Documentation Updates 175
Product Compatibility 179

Documentation Updates

IN THIS SECTION

- [New Simplified Documentation Architecture | 175](#)

This section lists the errata and changes in Junos OS Release 18.1R2 for the NFX Series documentation.

New Simplified Documentation Architecture

- With the release of Junos OS Release 18.1, Juniper is simplifying its technical documentation to make it easier for you to find information and know that you can rely on it when you find it. In the past, we organized documentation about Junos OS software features into platform-specific documents. In many cases, features are supported on multiple platforms, so you might not easily find the document you want for your platform.

With Junos OS Release 18.1, we have eliminated the platform-specific software feature documents. For example, if you want to find documentation on OSPF, there is only one document regardless of which platform you have. Here are some of the benefits of our new simplified architecture:

- Over time, you will see better search results when looking for Juniper documentation. You will be able to find what you want faster and be assured that is the right document.
- If a software feature is supported on multiple platforms, you can find information about all the platforms in one place.
- Because we have eliminated many documents that covered similar topics, you will now find one document with all the information.
- You can know that you are always getting the most current and accurate information.

SEE ALSO

[New and Changed Features | 163](#)

[Changes in Behavior and Syntax | 167](#)

[Known Behavior | 168](#)

[Known Issues | 170](#)

[Resolved Issues | 173](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases | 176
- Basic Procedure for Upgrading to Release 18.1 | 176

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.

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

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

Basic Procedure for Upgrading to Release 18.1

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

NOTE: The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the 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 18.1R2 on NFX250 devices:

1. Using a Web browser, navigate to the NFX250 software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/?p=nfx250#sw>
2. Select the release number (the number of the software version that you want to download) from the **Version** drop-down list to the right of the Download Software page.
3. In the **Install Package** section of the **Software** tab, select the software package for the release.
4. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
5. Review and accept the End User License Agreement.
6. Download the software to a local host.
7. Copy the software to the device or to your internal software distribution site.
8. Install the new package on the device. Use the following command to install the package:

```
root@jdm>request system software add
source/jinstall-host-nfx-2-flex-x86-64-18.1R2-secure-signed.tgz reboot
```

Replace **source** with the path name of the local directory on the device, for example, `/var/tmp`.

Adding the reboot command reboots the device after the upgrade is validated and installed. When the reboot is complete, the device 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 18.1R2 jinstall package, you cannot return to the previously installed software by issuing the **request system software rollback** command.

To download and install Junos OS Release 18.1R2 on NFX150 devices:

1. Using a Web browser, navigate to the NFX150 software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/?p=nfx150#sw>
2. Select the release number (the number of the software version that you want to download) from the **Version** drop-down list to the right of the Download Software page.
3. In the **Install Package** section of the **Software** tab, select the software package for the release.
4. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
5. Review and accept the End User License Agreement.
6. Download the software to a local host.
7. Copy the software to the device or to your internal software distribution site.
8. Install the new package on the device. Use the following command to install the package:

```
root@nfx150>request vmhost software add  
source/jinstall-host-nfx-3-x86-64-18.1R2.4-secure-signed.tgz reboot
```

Replace **source** with the path name of the local directory on the device, for example, /var/public.

Adding the reboot command reboots the device after the upgrade is validated and installed. When the reboot is complete, the device 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 18.1R2 jinstall package, you cannot return to the previously installed software by issuing the **request system software rollback** command.

SEE ALSO

[New and Changed Features | 163](#)

[Changes in Behavior and Syntax | 167](#)

[Known Behavior | 168](#)

[Known Issues | 170](#)

[Resolved Issues | 173](#)

[Documentation Updates | 175](#)

[Product Compatibility | 179](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 179](#)
- [Software Version Compatibility | 180](#)

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 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](#).

Software Version Compatibility

This section lists the vSRX and Cloud CPE Solution software releases that are compatible with the Junos OS releases on the NFX150 and NFX250 platforms:

NFX150 Software Version Compatibility

This section lists the vSRX software releases that are compatible with the Junos OS releases on the NFX150 platform:

Table 1: Software Compatibility Details with only vSRX Installed

NFX150 Junos OS Release	vSRX
18.1R1	18.1R1
18.1R2	18.1R2

NFX250 Software Version Compatibility

This section lists the vSRX and Cloud CPE Solution software releases that are compatible with the Junos OS releases on the NFX250 platform:

Table 2: Software Compatibility Details with vSRX and Cloud CPE Solution

NFX250 Junos OS Release	vSRX	Cloud CPE Solution
15.1X53-D40.3	15.1X49-D40.6	Cloud CPE Solution 2.0
15.1X53-D41.6	15.1X49-D61	Cloud CPE Solution 2.1
15.1X53-D102.2	15.1X49-D61	Cloud CPE Solution 3.0
15.1X53-D47.4	15.1X49-D100.6	Cloud CPE Solution 3.0.1
15.1X53-D490	15.1X49-D143	Cloud CPE Solution 4.0
15.1X53-D495	15.1X49-D160	Cloud CPE Solution 4.1

Table 3: Software Compatibility Details with only vSRX Installed

NFX250 Junos OS Release	vSRX
15.1X53-D40.3	15.1X49-D40.6
15.1X53-D41.6	15.1X49-D40.6
15.1X53-D45.3	15.1X49-D61
15.1X53-D47.4	15.1X49-D78.3
17.2R1	15.1X49-D75
17.3R1	15.1X49-D100
15.1X53-D471	15.1X49-D143
18.1R1	18.1R1
18.1R2	18.1R2

SEE ALSO

New and Changed Features 163
Changes in Behavior and Syntax 167
Known Behavior 168
Known Issues 170
Resolved Issues 173
Documentation Updates 175

Junos OS Release Notes for PTX Series Packet Transport Routers

IN THIS SECTION

- New and Changed Features | 182
- Changes in Behavior and Syntax | 190
- Known Behavior | 193
- Known Issues | 194
- Resolved Issues | 196
- Documentation Updates | 201
- Migration, Upgrade, and Downgrade Instructions | 202
- Product Compatibility | 206

These release notes accompany Junos OS Release 18.1R2 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/software/junos/>.

New and Changed Features

IN THIS SECTION

- Release 18.1R2 New and Changed Features | 183
- Release 18.1R1 New and Changed Features | 183

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 18.1R2 New and Changed Features

There are no new features or enhancements to existing features for PTX Series in Junos OS Release 18.1R2.

Release 18.1R1 New and Changed Features

Hardware

- **New Routing Engine RE-PTX-X8-128G (PTX5000)**—Starting in Junos OS Release 18.1R1, the RE-PTX-X8-128G Routing Engine is supported on the PTX5000 packet transport router. The Routing Engine has increased memory and storage to support node virtualization in future releases. The Routing Engine is equipped with an 8-Core 2.3-GHz processor, 128-GB memory, and 200-GB SSDs and also supports Secure Boot for enhanced boot security.

Class of Service (CoS)

- **Support for explicit-null packet classification using the EXP value from MPLS explicit-null labels (PTX Series)**—The default classification for explicit-null packets is based on the payload (IPv4 or IPv6 DSCP bits). Starting with Junos OS 18.1R1, PTX Series routers with third-generation FPCs (FPC3) support a new CLI option, `[explicit-null-cos inet|inet6]` at the `[edit forwarding-options]` hierarchy level, that makes the packet classification based on the MPLS EXP value rather than on the payload, thus preserving the MPLS classification of the packet.

[See [explicit-null-cos](#).]

- **Support for enabling a queue's buffer space to be 100 percent of the interface's buffer space (PTX Series)**—Starting in Junos OS 18.1R1, PTX Series devices provide a new CLI option that enables you to set a queue's buffer to be up to 100 percent of the interface's buffer. This option allows the queue's buffer to grow as large as 100 percent of the interface's buffer if and only if it is the only active queue for the interface. This option can be enabled by setting `buffer-size shared` at the `[edit class-of-service schedulers scheduler-name]` hierarchy level.

[See [buffer-size \(Schedulers\)](#).]

Interfaces and Chassis

- **Support for the removal of child next-hop usage for aggregated Ethernet Interfaces and clients (PTX Series routers with FPC3-PTX-U2 and FPC3-PTX-U3)**—Starting in Junos OS Release 18.1R1, Junos OS supports removal of child next-hop usage for aggregated Ethernet Interfaces and clients. Removal of child next-hop usage helps reduce the memory and CPU resources required to support aggregated Ethernet Interfaces and improves the overall system performance and scaling numbers. This feature is enabled by default if the network services mode on the router is configured to `enhanced-mode`. You can disable this feature by using the `set chassis aggregated-devices disable-lag-enhanced`. You must reboot the router for the configuration to take effect.

Previously, each unicast next hop over aggregated Ethernet Interfaces resulted in creation of a number of children next hops as well. For an aggregated Ethernet Interface with 16 member links, addition of one unicast next hop over the aggregated Ethernet Interface results in installing total of 17 next hops.

As a result, with aggregated Ethernet configuration, the number of next hops supported decreases in proportion to the number of aggregated Ethernet links.

NOTE: Child next-hop optimizations are supported for aggregated Ethernet interfaces, interfaces that make use of aggregated Ethernet interfaces, and for both unicast and multicast scenarios.

[See [Aggregated Ethernet Interfaces Overview](#).]

- **Upgraded SSD size and RAM size (PTX5000)**—Starting in Junos OS Release 18.1R1, PTX5000, routers with the RE-PTX-X8-128G-S Routing Engine support Secure Boot BIOS. The SSD size and the RAM size of the Routing Engine is upgraded to 2x200 GB and 128 GB.

[See [Salient Features of the Routing Engines with VM Host Support](#).]

Junos OS XML API and Scripting

- **SLAX and Python scripts now can be sourced over the non-default VRF management instance (PTX Series)**—Starting in Junos OS Release 18.1R1, configuration of commit, event, JET, op, and SNMP scripts is upgraded to support the non-default management routing instance **mgmt_junos** as an option when specifying the source URL for refreshing or downloading SLAX and Python scripts.

[See [Using an Alternate Source Location for a Script](#) or [Configuring and Using a Master Source Location for a Script](#).]

Management

- **Enhancement to NPU memory sensors for Junos Telemetry Interface (PTX Series)**—Starting with Junos OS Release 18.1R1, the format of telemetry data exported through gRPC for NPU memory and memory utilization implements prefix compression. This change reduces the payload size of data exported. The following example shows the new format:

key: __prefix__

str_value: /components/component[name='FPC0:NPU0']/properties/property

key: [name='mem-util-edmem-size']/value

uint_value: 12345

Telemetry data is exported in key-value pairs. Previously, the data exported included the component and property names in a single key string.

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

- **Physical interface operational status sensor (int-exp) support on Junos Telemetry Interface (JTI) (PTX Series)**—Starting with Junos OS Release 18.1R1, sensor int-exp (interface express) is supported to export interface operational **UP** and **DOWN** status at a user-configurable rate. This sensor leverages statistics out of the physical interface sensor, providing faster and more frequent operational status statistics. Only the physical interfaces' operational status from the Flexible PIC Concentrator (FPC) is collected and reported. Statistics from the Routing Engine interface are not reported.

You can apply the `intf-exp` sensor using the following paths:

- Subscription path

`/junos/system/linecard/intf-exp/`

- OpenConfig path

`/interfaces_exp/interface_exp[name='et-x/y/z:ch']/state/oper-statusdetails`

Streaming telemetry data through gRPC requires you to download the OpenConfig for Junos OS module.

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

- **Expanded support for chassis sensors for Junos Telemetry Interface (MX Series and PTX3000 and PTX5000 Transport Series Routers)**—Starting with Junos OS Release 18.1R1, Junos Telemetry Interface (JTI) provides new sensors that expand optics and power information.

To export telemetry data from Juniper equipment to an external collector requires both Junos Telemetry Interface (JTI) and gRPC to be configured.

Enhanced sensor information is also supported through operational mode commands **show chassis fpc detail**, **show chassis power detail**, and **show chassis pic fpc-slot id pic-slot id**.

Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module.

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

- **“ON CHANGE” sensor support through gRPC Network Management Interface (gNMI) for Junos Telemetry Interface (MX Series) (PTX Series)**—Starting with Junos OS Release 18.1R1, ON_CHANGE streaming of Address Resolution Protocol (ARP), Network Discovery Protocol (NDP), and IP sensor information associated with interfaces is supported on Junos Telemetry Interface (JTI).

Periodical streaming of OpenConfig operational states and counters has been supported since Junos OS Release 16.1, exporting telemetry data from Juniper equipment to an external collector. While useful in collecting all the needed information and creating a baseline “snapshot,” periodical streaming is less useful for time-critical missions. In such instances, you can configure ON_CHANGE streaming for an external collector to receive information only when operational states experience a change in state.

To support ON_CHANGE streaming, Google has developed a new specification called gRPC Network Management Interface (gNMI) for the modification and retrieval of configurations from a network element. Additionally, the gNMI specification can be used to generate and control telemetry streams from a network element to a data collection system. Using the new gNMI specification, one gRPC service definition can provide a single implementation on a network element for both configuration and telemetry as well as a single NMS element to interact with a device by means of telemetry and configuration RPCs.

Information about the RPCs supporting this feature can be found in the gNMI Proto file version 0.4.0 (the supported version) and the specification released by Google at:

- <https://github.com/openconfig/reference/blob/master/rpc/gnmi/gnmi-specification.md>
- <https://github.com/openconfig/gnmi/blob/master/proto/gnmi/gnmi.proto>

The telemetry RPC **subscribe** under gNMI service supports ON_CHANGE streaming. RPC **subscribe** allows a client to request the target to send it values of particular paths within the data tree. Values may be streamed (STREAM), sent one-off on a long-lived channel (POLL), or sent one-off as a retrieval (ONCE).

If a subscription is made for a top level container with a sample frequency of 0, leaves with ON_CHANGE support are streamed based on events. Other leaves will not be streamed.

NOTE: In order to permit a device to decide which nodes will be streamed as ON_CHANGE and which will SAMPLE, the collector should subscribe for TARGET_DEFINED with sample_interval.

Streaming telemetry data through gRPC requires you to download the OpenConfig for Junos OS module.

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

- **ON_CHANGE support for Junos Telemetry Interface (JTI) (PTX Series)**—Starting with Junos OS Release 18.1R1, OpenConfig support through gRPC Remote Procedure Calls (gRPC) and JTI is extended to support client streaming and bidirectional streaming of telemetry sensor information.

APIs have been implemented in Junos based on Protobuf specifications released by Google for OpenConfig. These APIs perform configuration, operational state retrieval, and telemetry on Junos routers using gRPC as the transport mechanism.

Starting in Junos OS 18.1R1, client streaming and bidirectional streaming are supported. With client streaming, the client sends a stream of requests to the server instead of a single request. The server typically sends back a single response containing status details and optional trailing metadata. With bidirectional streaming, both client and server send a stream of requests and responses. The client starts the operation by invoking the RPC and the server receives the client metadata, method name, and deadline. The server can choose to send back its initial metadata or wait for the client to start sending requests. The client and server can read and write in any order. The streams operate completely independently.

Junos devices can be managed through API (RPC) prototypes:

- **rpc Capabilities (CapabilityRequest)**

Returns (CapabilityResponse). Allows the client to retrieve the set of capabilities that is supported by the target.

- **rpc Get (GetRequest)**

Returns (GetResponse). Retrieves a snapshot of data from the target.

- **rpc Set (SetRequest)**

Returns (SetResponse). Allows the client to modify the state of data on the target.

- **rpc Subscribe (stream SubscribeRequest)**

Returns (stream SubscribeResponse). Allows a client to request the target to send it values for particular paths within the data tree. These values may be streamed (STREAM) or sent one-off on a long-lived channel (POLL), or sent as a one-off retrieval (ONCE). If a subscription is made for a top-level container with a sample frequency of 0, leaves with ON_CHANGE support are streamed based on events. Other leaves will not be streamed.

Juniper Extension Toolkit (JET) support provides insight to users regarding the status of clients connected to JSD. JET support for gRPC includes expanding the maximum number of clients that can connect to JSD from 8 to 30 (the default remains 5). To specify the maximum number of connections, include the **max-connections** statement at the **[edit system services extension-service request-response grpc]** hierarchy level.

To provide information regarding the status of clients connected to JSD, issue the enhanced **show extension-service client information** command and include the **clients** or **servers** options. The **clients** option displays request-response client information. The **servers** option displays request-response server information.

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

MPLS

- **Support for static adjacency segment identifier for aggregated Ethernet member links (PTX Series)**—Starting with Junos OS Release 18.1R1, you can configure a transit single-hop static label switched path (LSP) for a specific member link of an aggregated Ethernet (AE) interface, without enabling the **enhanced-ip** network services mode. A static labeled route is added with next-hop pointing to the AE member link of an aggregated interface. Label for these routes is picked from the segment routing local block (SRLB) pool of the configured static label range. This feature is supported for AE interfaces on PTX routers with FPC1, FPC2, and FPC3. The member-interface CLI statement is added under transit configuration to configure the AE member interface name. The static LSP label is configured from defined static label range.

NOTE:

- In the previous release, this feature was supported only when the **enhanced-ip** network services mode was enabled.
- If the ingress port for the OAM traffic is on FPC1 or FPC2, and the egress port (member link) has the Link Aggregation Control Protocol (LACP) Mux state as 'Detached', and the corresponding physical port (on FPC1, FPC2, or FPC3) is up, the traffic is forwarded at ingress.

[See [Configuring Static Adjacency Segment Identifier for Aggregate Ethernet Member Links Using Single-hop Static LSP](#).]

- **Support for segment routing statistics at the ingress (PTX Series)**— Starting in Junos OS Release 18.1R1, the traffic statistics in a segment routing (SR) network can be recorded in an OpenConfig compliant

format for Layer 3 interfaces. The statistics is recorded at the ingress for the Source Packet Routing in Networking (SPRING) traffic only, excluding RSVP and LDP-signaled traffic, and the family MPLS statistics per interface is accounted for separately. The SR statistics also includes SPRING traffic statistics per link aggregation group (LAG) member, and per segment identifier (SID).

To enable recording of SR statistics, include the **sensor-based-stats per-interface-per-member-link ingress** statement at the **[edit protocols isis source-packet-routing]** hierarchy level.

[See [per-interface-per-member-link](#).]

Network Management and Monitoring

- **Enhancement to Junos OS SNMP MIB PCC functionality (PTX Series)**—Starting in Junos OS Release 18.1R1, Junos OS provides enhanced MIB support for Path Computation Clients. This enhancement enables the Path Computation Client (PCC) process to accept SNMP **get** and **getnext** commands for Path Computation Client Protocol (PCEP) peer and PCEP session tables and reply to them. This feature monitors PCEP interactions between a PCC and a Path Computation Element (PCE). Not all members of PCEP peer and PCEP session tables mentioned in the RFC (RFC 7420) are supported. For exceptions, see [Standard SNMP MIBs Supported by Junos OS](#).

[See [MIB Explorer](#). Name of MIB is **pcep.mib**.]

Routing Policy and Firewall Filters

- **Filter-based GRE encapsulation (PTX Series)**—Starting with Junos OS Release 18.1R1, for PTX Series routers running third-generation line cards, you can use **tunnel-end-point** commands to enable line-rate, filter-based, GRE tunneling of IPv4 and IPv6 payloads across IPv4 networks.

This GRE encapsulation is not supported for logical systems, or for MPLS traffic, and the route lookup for GRE encapsulated traffic is supported on the default routing instance only.

The following commands are introduced for this feature:

set firewall tunnel-end-point *tunnel-name* gre.

set firewall tunnel-end-point *tunnel-name* ipv4.

set firewall tunnel-end-point *tunnel-name* ipv6.

[See [tunnel-end-point](#) and [Filter-Based Tunneling Across IPv4 Networks](#).]

- **Firewall filter enhancement for better resource optimization (PTX Series)**—When an interface specific firewall filter is configured with multiple Interface bind point instances, the PTX Series Help software allocates resources for each interface instance separately, and the resources consumption is directly proportional to the number of bind points. For better resource optimization, a new **scale-optimized** configuration statement is introduced starting in Junos OS Release 18.1R1 that optimizes interface specific firewall filters in the Packet Forwarding Engine itself. The ingress and egress traffic cannot have the same scale-optimized filter configured.

For more information, see [Guidelines for Configuring Firewall Filters](#).

Routing Protocols

- **Support for BGP multipath at global level (PTX Series)**—Starting with Junos OS Release 18.1R1, BGP multipath is available at the global level in addition to the group and neighbor level. In earlier Junos OS releases BGP multipath is supported only at the group and neighbor levels. A new configuration option **disable** is available at the **[edit protocols bgp multipath]** hierarchy level to disable BGP multipath for specific groups or neighbors. This allows you to configure BGP multipath globally and disable it for specific groups according to your network requirements.

[See [disable](#).]

Security

- **Secure Boot (PTX5000 with Routing Engine RE-PTX-X8-128G)**—Starting in Junos OS Release 18.1R1, 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 and thus safeguarded from tampering or modification. By default, Secure Boot is enabled on supported routers.

[See [Feature Explorer](#) and enter **Secure Boot**.]

Services Applications

- **Support for MPLS-over-UDP inner payload flow monitoring with IPFIX and version 9 formats (PTX Series)** —Starting with Junos OS Release 18.1R1 on PTX Series routers with an FPC3, PTX10K-LC1101, PTX10K-LC1102, or PTX1000 card, you can perform flow monitoring for MPLS-over-UDP flows to look past the tunnel header to sample and report on the inner payload at both the transit and egress nodes of the tunnel. This feature supports MPLS IPv4 and IPv6 payloads and both IPFIX and version 9 templates. Only ingress sampling is supported.

[See [Inline Active Flow Monitoring of MPLS-over-UDP Flows on PTX Series Routers](#).]

SEE ALSO

[Changes in Behavior and Syntax](#) | **190**

[Known Behavior](#) | **193**

[Known Issues](#) | **194**

[Resolved Issues](#) | **196**

[Documentation Updates](#) | **201**

[Migration, Upgrade, and Downgrade Instructions](#) | **202**

[Product Compatibility](#) | **206**

Changes in Behavior and Syntax

IN THIS SECTION

- [Interfaces and Chassis | 190](#)
- [Management | 192](#)
- [Network Management and Monitoring | 192](#)
- [Network Operations and Troubleshooting Automation | 192](#)

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 18.1R2 for the PTX Series.

Interfaces and Chassis

- **Modified output of the request vmhost zeroize command**—The command **request vmhost zeroize**, upon execution, prompts the user for confirmation to proceed. The following line is displayed:

```
user@host request vmhost zeroize
VMHost Zeroization : Erase all data, including configuration and log files ?
[yes,no] (no) yes
```

See [request vmhost zeroize](#).

- **Power supply alarm is not raised when the input switch status is OFF or power not connected (PTX10008, PTX10016)**—Starting in Junos OS release 17.4R2 and 18.1R2, the power supply alarm **A power supply input has failed** will not be raised if INP1/INP2 switch status is OFF and the power is not connected. Earlier, an alarm is raised for the Power Entry Module (PEM) that are not powered on as **Not Powered** irrespective of the switch state. Now, to know the power supply status, execute **show chassis power** or **show chassis power detail** CLI command. The **DC input** is the new output parameter that provides information about the status of the input feed.

Previous Behavior:

user@host> show chassis power

```
PEM 0:
  State:      Online
  Capacity:   2500 W (maximum 2500 W)
```

```

    DC output: 864 W (zone 0, 72 A at 12 V, 34% of capacity)

PEM 1:
  State:      Online
  Capacity:   2500 W (maximum 2500 W)
  DC output:  864 W (zone 0, 72 A at 12 V, 34% of capacity)

System:
  Zone 0:
    Capacity:      7500 W (maximum 7500 W)
    Allocated power: 6525 W (975 W remaining)
    Actual usage:   2616 W
    Total system capacity: 7500 W (maximum 7500 W)
    Total remaining power: 975 W

...

```

Current Behavior:

user@host> show chassis power

```

PEM 0:
  State:      Online
  Capacity:   2500 W (maximum 2500 W)
  DC input:   OK (No feed expected, Both feed connected)
  DC output:  576 W (zone 0, 48 A at 12 V, 23% of capacity)

PEM 1:
  State:      Online
  Capacity:   2500 W (maximum 2500 W)
  DC input:   OK (No feed expected, Both feed connected)
  DC output:  576 W (zone 0, 48 A at 12 V, 23% of capacity)

...

```

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

Management

- **Enhancement to LSP statistics sensor for Junos Telemetry Interface (PTX Series)**—Starting with Junos OS 18.1R1, the telemetry data exported for the LSP statistics sensor no longer includes the phrase **and source 0.0.0.0** after the LSP name in the value string for the prefix key. This change reduces the payload size of data exported. The following is an example of the new format:

```
str_value: /mpls/lsp/constrained-path/tunnels/tunnel[name='LSP-4-3']/state/
counters[name='c-27810']/
```

Network Management and Monitoring

- **SNMP syslog messages changed (PTX Series)**—In Junos OS Release 18.1R1, 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](#).]

Network Operations and Troubleshooting Automation

- **JET - Correction to escaped characters notification events (PTX Series routers)**—Per RFC7159, certain characters must be escaped. Data returned from JET notification subscriptions contained escaped characters that were not required. This has been corrected to comply with RFC7159.
- **respawn-on-normal-exit option added to [edit system extensions extension-service application file <application-name>] hierarchy (PTX Series routers)**—This option helps to ensure that daemonized Juniper Extension Toolkit (JET) applications that exit normally will restart without user intervention. Daemonized JET applications that exit unexpectedly will still restart without user intervention. This is the default behavior.

SEE ALSO

[New and Changed Features | 182](#)

[Known Behavior | 193](#)

[Known Issues | 194](#)

[Resolved Issues | 196](#)

[Documentation Updates | 201](#)

Known Behavior

IN THIS SECTION

- [General Routing | 193](#)
- [Interfaces and Chassis | 194](#)

This section contains the known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.1R2 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

- For CFP2-DCO-T-WDM-1 pluggable, Rx payload type is shown incorrectly (shown as 0 instead of 7). [PR1300423](#)
- When a CFP2-DCO-T-WDM-1 plugged in a PTX Series PIC, when backward frr is enabled on the far end the convergence time is higher because extra delay (average 500 msec) is incurred in the triggering FRR, because of SW-based polling. [PR1303820](#)
- EPR queue is not getting drained during FRR test, and the packets already in the queue timeout eventually, causing this interrupt. This is a minor alarm. [PR1319520](#)
- This is expected behavior for TQ-chip ASICs. It is primarily due to strict-high priority queue and the shared shaper. Credits that are unused by an Output Queue (that is, the queue actual rate is less than the tx-rates) will cause the queue's credit bucket to reach its maximum value. Once a queue hits its maximum credit value, the remaining credits will be distributed to other queues. Once the other queues get transmit credits, they can then transmit. Thus with TQ-chip and the shared shaper, it is virtually impossible to completely shut off a queue by means of a guaranteed rate mechanism. [PR1319923](#)

Interfaces and Chassis

- On PTX10008 and PTX10016 routers, if you remove the redundant Switch Interface Board (SIB) after upgrading Junos OS from Release 17.4R1 or Release 17.2X75-D90 to a later release, then an alarm is not generated. This is a known behavior and has no impact on the performance of the router.

SEE ALSO

[New and Changed Features | 182](#)

[Changes in Behavior and Syntax | 190](#)

[Known Issues | 194](#)

[Resolved Issues | 196](#)

[Documentation Updates | 201](#)

[Migration, Upgrade, and Downgrade Instructions | 202](#)

[Product Compatibility | 206](#)

Known Issues

IN THIS SECTION

- [General Routing | 195](#)
- [Infrastructure | 196](#)
- [Interfaces and Chassis | 196](#)
- [MPLS | 196](#)

This section lists the known issues in hardware and software in Junos OS Release 18.1R2 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

- When CFP2-DCO-T-WDM-1 plugged in a PTX Series packet transport router PIC, after repeated configuration rollbacks, the link can take a long time to come up. [PR1301462](#)
- When CFP2-DCO-T-WDM-1 plugged in a PTX Series packet transport router PIC, after FPC restart sometimes a carrier frequency offset TCA is raised even when TCA not enabled. [PR1301471](#)
- Internal latency is high during initial subscription of sensors when multiple sensors (in order of 15-20) are subscribed together. This issue is not observed with a lesser number of subscriptions, and it only occurs for a short period when sensors are being installed. [PR1303393](#)
- This type of crash indicates simultaneous operation on an ephemeral instance. When a process wants to open an ephemeral configuration in merge view, some other activity (like purging, deletion-recreation) is being carried out on this ephemeral instance. The occurrence of this core file is rare. [PR1305424](#)
- Change in output of **show chassis power** command for PTX10008 and PTX10016. [PR1311574](#)
- Whenever user changes pic or port speed an alarm is raised and user intervention is require to take the effect. [PR1311875](#)
- On PTX10000 100G LR4 optics with Part Number 740-061409 will show as QSFP-100G-LR4-T2 instead of QSFP-100G-LR4 and optics which shows as QSFP-100G-LR4 is not supported on PTX10000. [PR1322082](#)
- On PTX Series platforms with cards such as FPC1 and FPC2 and class of service (CoS) used, a high-priority queue might not get the entire configured bandwidth. [PR1324853](#)
- Filters configured with a scale-optimized command for pointing to traffic-class-count will not increment. [PR1334580](#)
- Disabling et-0/0/5:2 also disables et-0/0/5:0. This issue is due to incorrect qsfp28 optics channel and Broadcom retimer lane mapping. [PR1337975](#)
- The issue is with interoperability of TQ- chip with PTX Series routers based line cards. [PR1339481](#)
- In a rare case on PECHIP based PTX Series FPCs, DFE tuning can result in a port staying down. [PR1340612](#)
- The RHI interface on PTX Series packet transport routers can carry a maximum of 4-Mbps traffic on OQ1. Hence, NDP, which is mapped to OQ1 and a bandwidth assigned earlier of 500 pps is reduced to 100 pps due to this limitation. [PR1345938](#)
- In the event of Routing Engine switchover, if there are existing sensor subscriptions, they will continue to show in **show agent sensors** output after the switchover. These stale sensors will be cleared when the device becomes master again. [PR1347779](#)

Infrastructure

- A file system corruption might create a kernel core file. The Routing Engine reboots with the message `ffs_blkfree: freeing free block`. [PR1028972](#)

Interfaces and Chassis

- Junos OS upgrade involving Junos OS Release 14.2R5 (and later 14.2 maintenance releases) and Junos OS Release 16.1 (and later mainline releases) with CFM configuration can cause `cfmd` to crash after upgrade. This is due the old version of `/var/db/cfm.db`. [PR1281073](#)

MPLS

- When the `rpd` daemon is terminating, the process of signaling the deletion of all RSVP LSPs might take so long that a watchdog timer is firing, resulting in an `rpd` core file. [PR1257367](#)

SEE ALSO

New and Changed Features	 182
Changes in Behavior and Syntax	 190
Known Behavior	 193
Resolved Issues	 196
Documentation Updates	 201
Migration, Upgrade, and Downgrade Instructions	 202
Product Compatibility	 206

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 18.1R2](#) | [197](#)
- [Resolved Issues: 18.1R1](#) | [198](#)

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: 18.1R2

General Routing

- Remove **show chassis spmb** command/response. [PR1244059](#)
- De-encapsulated GRE traffic is not passing to the egress port upon initial customer configuration. [PR1325104](#)
- On PTX5000 line packet transport routers with FPC3 linecards, PTX10000 line, and PTX1000 line output firewall filters that are configured with **syslog** and **discard** actions do not perform the **syslog** action. [PR1328426](#)
- PTX10000 line card might reboot continuously after upgrading to Junos OS Release 17.2R1 or later if HMC BIST fails. [PR1330618](#)
- Traffic stops flowing out of ae70 after some FPC restart iterations. [PR1335118](#)
- Member of IPv4 unicast next hops might be stuck in "Replaced" state after interface flaps. [PR1336201](#)
- FPC/FPC2/FPC E on PTX Series does not forward traffic. [PR1339524](#)
- PTX1008: 30-Port Coherent Line Card (DWDM-IC) does not come up. [PR1344732](#)

Interfaces and Chassis

- On PTX3000 line, when CPM is configured, the CFM filter is not getting programmed. The command **show oam ethernet connectivity-fault-management** is not checking interfaces ae0.0 extensive. [PR1335305](#)

Platform and Infrastructure

- On PTX1000 and QFX10002-60C: Python scripts/shell scripts cannot be executed during ZTP because `verexec` is enabled. [PR1334425](#)

Routing Protocols

- The `rpd` might constantly consume high CPU in BGP setup. [PR1315066](#)
- The primary path of MPLS LSP might switch to another address. [PR1316861](#)
- On PTX1000, `rpd` core file is generated at `ispfc_incrementally_mend_one_postf_sp_tree (postf_spf_res= <optimized out>, topo= <optimized out>)` at `../../../../../../../../src/junos/usr/sbin/rpd/lib/igp-spf-compute/igp_spf_compute_ti_lfa.c:3364`. [PR1339296](#)

Resolved Issues: 18.1R1

General Routing

- **restart na-grpc-server** and **restart na-mqtt** for MTRE does not work. [PR1284121](#)
- Traffic passing LSP with entropy label might be dropped after the bypass path goes down. [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 front panel display on PTX Series routers. [PR1294741](#)
- **LINK LED** is red when the port is disabled on PTX Series routers. [PR1294871](#)
- Classifier binding for logical interface (IFL) is lost when changing from trunk to access with L2 classifier configured. [PR1295043](#)
- After deleting and re-adding an interface that had a classifier bound, the binding to the default classifier is not restored. [PR1295477](#)
- FPC might crash after Routing Engine switchover. [PR1296282](#)
- An 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](#)
- Upon configuring protect core, rpd keeps thrashing at rt_attrib.c - nhp->rtn_n_gw > 1 && nhp->rtn_n_gw <= 64. [PR1297044](#)
- 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](#)
- **Link errors** alarm messages might be seen after migrating to FPC3 on PTX3000. [PR1298841](#)
- The disable-pfe action upon Hybrid Memory Cube (HMC) fatal errors might have a system-wide impact on PTX Series platforms. [PR1300180](#)
- On PTX3000 platforms, powering on a FPC (PTX-IPLC-B-32) card might cause the other FPC cards to reboot. [PR1302304](#)
- The third-generation FPC (FPC3-SFF-PTX) might not boot on a PTX3000 with the Control Board or Routing Engine. [PR1303295](#)
- On PTX3000 and PTX5000 platforms, the 100G interfaces might not come up. [PR1303324](#)
- If MPLS LSP self-ping is enabled (self-ping is enabled by default), the kernel might panic with the error message **Fatal trap 12: page fault while in kernel mode**. [PR1303798](#)

- Repeated log messages `%PFE-3 fpcX expr_nh_index_tree_ifl_get` and `expr_nh_index_tree_ipaddr_get` are observed when the sampling packet is discarded with `log` (or `syslog`) command under the firewall filter. [PR1304022](#)
- The **interface hold-time down** timer does not take effect on PTX5000 with optical interface. [PR1307302](#)
- Packet Forwarding Engine error messages are flooding as `expr_sensor_update_cntr_to_sid_tree` after deleting and rolling back **protocols isis source-packet-routing node-segment**. [PR1309288](#)
- After ZTP gets completed, the configuration on the backup Routing Engine is rolled back to the factory-default configuration in a few minutes. [PR1310117](#)
- The **SIB LED** on the FPD goes to green steady state even before an SIB comes online. [PR1311632](#)
- PTX Series routers might fail to grab a new region for the next hop during a link flap. [PR1311850](#)
- Rpd core observed after multiple session flaps on scale setup. [PR1312169](#)
- The 10g interface might flap if it is set to 100g speed. [PR1315079](#)
- Continuous logs from `vhclient` are seen for all the commands executed. [PR1315128](#)
- ZTP config file fails to be loaded and committed, Cannot open configuration file `/config/auto_image_upgrade.conf`. [PR1315857](#)
- The physical interfaces (IFDs) might generate framing errors when ports are connected to an odd interface. [PR1317827](#)
- After jack-out/jack-in FPCs show "No-Power" for some time; however, FPCs eventually come up. [PR1319156](#)
- No traffic is flowing with IPV6 payload prefixes on PTX Series platform. [PR1319273](#)
- The rpd might crash when OpenConfig package is upgraded with JTI streaming data in the background. [PR1322553](#)
- The aggregated Ethernet interface might be in an error blocked state after enabling and disabling aggregated Ethernet member link in a large scale of routes scenario. [PR1323398](#)
- Fan tray 0(FAN-PTX-V-S) Failure alarm is set and cleared on multiple PTX Series routers. [PR1324905](#)
- On PTX1000, the local time on FPC might be different from the local time on Junos VM host. [PR1325048](#)
- Firewall filter is not supported on aggregated Ethernet. [PR1325237](#)
- On PTX5000 w/ FPC3 linecards, PTX10000, and PTX1000 platforms, output firewall filters that are configured with "syslog" and "discard" actions do not perform the "syslog" action. [PR1328426](#)
- Sensor configuration is not deleted from ephemeral database after collector disconnects. [PR1329134](#)
- Additional TX reset during link-down events can cause link instabilities. [PR1330708](#)
- PTX FPC might reboot in certain rare scenarios when an flapping interface configuration is committed. [PR1335161](#)

Infrastructure

- ixlv interface statistics not accounting properly. [PR1313364](#)
- PTX device may get to abnormal state due to the malfunction of the protection mechanism for F-Label. [PR1336207](#)

Interfaces and Chassis

- The transportd might crash when SNMP 1335438query on jnxoptIfOChSinkCurrentExtTable with unsupported interface index. [PR1335438](#)

MPLS

- Traffic drop occurs during NSR switchover for RSVP P2MP provider tunnels used by MVPN. [PR1293014](#)
- Traffic loss occurs for static LSP configured with the **stitch** command. [PR1307938](#)
- Rpd crashes on backup Routing Engine due to memory exhaustion. [PR1328974](#)

Platform and Infrastructure

- Continuous log messages occur: for example: **tftpd[23724]: Timeout #35593 on DATA block 85.** [PR1315682](#)
- PTX1000 & QFX10002-60C: Python scripts/shell scripts cannot be executed during ZTP as veriexec is enabled. [PR1334425](#)

Routing Protocols

- With BGP LU FRR in an inter-AS scenario, a very high FRR time is visible once the link is up. [PR1307258](#)
- Assignment of Sub-TLV values for segment routing TE policy Sub-TLVs occurs. [PR1315486](#)
- The rpd process might crash continuously on both Routing Engines when "backup-spf-options remote-backup-calculation" is configured in IS-IS protocol. [PR1326899](#)

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 flaps repeatedly. [PR1282875](#)

SEE ALSO

[New and Changed Features | 182](#)

[Changes in Behavior and Syntax | 190](#)

[Known Behavior | 193](#)

[Known Issues | 194](#)

[Documentation Updates | 201](#)

Documentation Updates

IN THIS SECTION

- [New Simplified Documentation Architecture | 201](#)

This section lists the errata and changes in Junos OS Release 18.1R2 documentation for the PTX Series.

New Simplified Documentation Architecture

- With the release of Junos OS Release 18.1, Juniper is simplifying its technical documentation to make it easier for you to find information and know that you can rely on it when you find it. In the past, we organized documentation about Junos OS software features into platform-specific documents. In many cases, features are supported on multiple platforms, so you might not easily find the document you want for your platform.

With Junos OS Release 18.1, we have eliminated the platform-specific software feature documents. For example, if you want to find documentation on OSPF, there is only one document regardless of which platform you have. Here are some of the benefits of our new simplified architecture:

- Over time, you will see better search results when looking for Juniper documentation. You will be able to find what you want faster and be assured that is the right document.
- If a software feature is supported on multiple platforms, you can find information about all the platforms in one place.
- Because we have eliminated many documents that covered similar topics, you will now find one document with all the information.
- You can know that you are always getting the most current and accurate information.

SEE ALSO

[Known Behavior | 193](#)

[Known Issues | 194](#)

[Resolved Issues | 196](#)

[Migration, Upgrade, and Downgrade Instructions | 202](#)

[Product Compatibility | 206](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 202](#)
- [Upgrading a Router with Redundant Routing Engines | 203](#)
- [Basic Procedure for Upgrading to Junos OS Release 18.1 | 203](#)

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 17.1, 17.2 and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

Upgrading a Router with Redundant Routing Engines

If the router has two Routing Engines, perform 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 acting as the backup Routing Engine.

For the detailed procedure, see the [Installation and Upgrade Guide](#).

Basic Procedure for Upgrading to Junos OS Release 18.1

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 18.1R2:

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/>
2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.
4. Select the **Software** tab.
5. In the **Install Package** section of the **Software** tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by 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 18.1R2 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-18.1R2.SPIN-domestic-signed.tgz
```

All other customers, use the following command:

```
user@host> request system software add validate reboot  
source/jinstall-18.1R2.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 18.1 **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	 182
Changes in Behavior and Syntax	 190
Known Behavior	 193
Known Issues	 194
Resolved Issues	 196
Documentation Updates	 201
Product Compatibility	 206

Product Compatibility

IN THIS SECTION

●	Hardware Compatibility	 206
---	--	-----------------------

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	 182
Changes in Behavior and Syntax	 190
Known Behavior	 193
Known Issues	 194
Resolved Issues	 196
Documentation Updates	 201
Migration, Upgrade, and Downgrade Instructions	 202

Junos OS Release Notes for the QFX Series

IN THIS SECTION

- [New and Changed Features](#) | [208](#)
- [Changes in Behavior and Syntax](#) | [227](#)
- [Known Behavior](#) | [229](#)
- [Known Issues](#) | [234](#)
- [Resolved Issues](#) | [240](#)
- [Documentation Updates](#) | [248](#)
- [Migration, Upgrade, and Downgrade Instructions](#) | [249](#)
- [Product Compatibility](#) | [263](#)

These release notes accompany Junos OS Release 18.1R2 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Caveat: Juniper Networks does not recommend configuring and deploying EVPN-VXLAN on QFX Series platforms running Junos OS 18.1R1.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at <https://www.juniper.net/documentation/software/junos/>.

New and Changed Features

IN THIS SECTION

- [Release 18.1R2 New and Changed Features | 208](#)
- [Release 18.1R1 New and Changed Features | 209](#)

This section describes the new features for the QFX Series switches in Junos OS Release 18.1R2.

NOTE: The following QFX Series platforms are supported in Release 18.1R2: QFX5100, QFX5110, QFX5200, QFX5210, QFX10002, QFX10008, and QFX10016.

Release 18.1R2 New and Changed Features

EVPNs

- **IPv4 inter-VLAN multicast forwarding modes for EVPN (QFX10000 switches)**—Starting with Junos OS Release 18.1R2, 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.

Restoration Procedures and Failure Handling

- **Device recovery mode introduced in Junos OS with upgraded FreeBSD (QFX Series)**—In Junos OS Release 18.1R2, 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](#).]

Release 18.1R1 New and Changed Features

Hardware

- **QFX10002-60C switch**—Starting in Junos OS Release 18.1R1, Juniper Networks introduces the QFX10002-60C switch. The Juniper Networks QFX10000 line of Ethernet switches provides cloud builders and data center operators with scalable solutions for both core and spine data center deployments. The 2 U fixed-configuration switch has 60 flexible configuration speed ports that can be set for 40-Gbps or 100-Gbps speeds. The QFX10002-60C also supports 10-Gigabit Ethernet when the ports are configured for 40-Gigabit Ethernet and channelized into 4 independent 10-Gigabit Ethernet ports. The QFX10002-60C is available with either AC or DC power supplies. The airflow is airflow out, where air comes into the vents in the port panel and exhausts through the field-replaceable units (FRU) panel. [See [QFX10002 Hardware Overview](#).]
- **QFX5210-64C switch**—Starting in Junos OS Release 18.1R1, Juniper Networks introduces the QFX5210-64C Switch. The 1 U fixed configuration switch is designed for cloud customers who need either a top-of-rack switch or a lean spine switch with flexible port speeds and high-port density. The Routing Engine and control plane are driven by the 2.2 GHz quad-core Intel; Xeon; CPU with 16 GB of memory and a 128-GB solid-state drive (SSD) for storage. The QFX5210-64C can be configured for

10/25/40/50/100 Gigabit Ethernet speeds. The switch comes standard with redundant fans and redundant power supplies. The QFX5210-64C can be ordered with either ports-to-FRUs or FRUs-to-ports airflow. The model is available with either AC or DC power supplies.

- **QFX5200-48Y switch**— The Juniper Networks QFX5200 line of fixed-configuration access switches are designed for cloud builders and data centers deploying next-generation IP fabric networks. The QFX5200-48Y offers 48 ports of native 25-Gbps speed for downlinks and 6 ports of 100-Gbps speeds for uplinks. The 1 U fixed chassis switch allows a flexible configuration of the ports. The 40 downlink ports can be configured either as 10-Gbps speeds or 25-Gbps speeds while the 6 uplink ports can be configured for either 40-Gbps speeds or 100-Gbps speeds. The QFX5200-48Y comes standard with redundant fans and redundant power supplies. The QFX5200-48Y can be ordered with either ports-to-FRUs (AFO) or FRUs-to-ports (AFi) airflow. The model is available with either AC or DC power supplies.

[See [QFX5200 Switch Hardware Guide](#).]

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

- **Access control and authentication (QFX5100 switches)**—Starting with Junos OS Release 18.1 R1, QFX5110 and QFX5200 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 authenticate 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.

[See [Understanding Authentication on Switches.](#)]

Class of Service

- **Support for data center quantized congestion notification (DCQCN) (QFX5100, QFX5110, QFX5200, QFX5210 switches)**—Remote Direct Memory Access (RDMA) provides the high throughput and ultra-low latency, with low CPU overhead, necessary for modern datacenter applications. RDMA is deployed using the RoCEv2 protocol, which relies on priority-based flow control (PFC) to enable a drop-free network. DCQCN is an end-to-end congestion control scheme for RoCEv2. Starting in Junos OS Release 18.1R1, Junos OS supports DCQCN by combining explicit congestion notification (ECN) and PFC to overcome the limitations of PFC to support end-to-end lossless Ethernet.

[See [Data Center Quantized Congestion Notification \(DCQCN\).](#)]

EVPN

- **Support for IGMP snooping for EVPN-VXLAN in a multihomed environment (QFX5110 switches)**—Starting in Junos OS Release 18.1R1, QFX5110 switches support IGMP snooping with Ethernet EVPN (EVPN). This feature is useful in an EVPN-VXLAN environment with significant multicast traffic. IGMP snooping enables PE devices to send multicast traffic to CE devices only as needed, which preserves bandwidth. To configure IGMP snooping, include the **igmp-snooping (all | vlan-number)** set of statements at the **[edit protocols]** hierarchy level. You must also include the proxy statement in the IGMP snooping configuration. All multihomed interfaces must have the same configuration.

[See [Overview of IGMP Snooping in an EVPN-VXLAN Environment.](#)]

- **EVPN control plane and VXLAN data plane support (QFX5210 switches)**—By using a Layer 3 IP-based underlay network coupled with an Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) overlay network, you can deploy larger networks than those possible with traditional Layer 2 Ethernet-based architectures. With overlay networks, endpoints (bare-metal servers [BMSs] and virtual machines [VMs]) can be placed anywhere in the network and can remain connected to the same logical Layer 2 network, enabling the virtual topology to be decoupled from the physical topology.

The physical underlay network over which EVPN-VXLAN is commonly deployed is a two-layer IP fabric, which includes spine and leaf devices. The spine devices provide connectivity between the leaf devices, and the leaf devices function as Layer 2 VXLAN gateways and provide connectivity to the attached endpoints. Starting with Junos OS Release 18.1R1, you can deploy QFX5210 switches as leaf nodes in the EVPN-VXLAN overlay network.

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

- **EVPN proxy ARP and ARP suppression, and NDP and NDP suppression with or without IRB interfaces (QFX5100, QFX5110, and QFX5200 switches)**—Starting with Junos OS Release 18.1R1, QFX5100 and QFX5200 switches that function as Layer 2 VXLAN gateways and QFX5110 switches that function as Layer 2 or Layer 3 VXLAN gateways in an Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) environment support proxy Address Resolution Protocol (ARP) and ARP suppression, and Network Discovery Protocol (NDP) and NDP suppression. The proxy ARP and ARP suppression, and NDP and

NDP suppression capabilities are enabled by default. Any interface configured on a Layer 2 or Layer 3 VXLAN gateway can deliver ARP requests from both local and remote hosts.

In addition, you can control the following aspects of the media access control (MAC)-IP address bindings database on a Layer 2 or Layer 3 VXLAN gateway:

- The maximum number of MAC-IP address entries in the database
- The amount of time a locally learned MAC-IP address binding remains in the database

[See [EVPN Proxy ARP and ARP Suppression, and NDP and NDP Suppression](#).]

- **Support for duplicate MAC address detection and suppression (QFX5100, QFX5110, and QFX5200 switches)**— When a MAC address relocates, PE devices can converge on the latest location by using sequence numbers in the extended community field. Misconfigurations in the network can lead to duplicate MAC addresses. Starting in Junos OS Release 18.1R1, QFX5100, QFX5110, and QFX5200 switches support duplicate MAC address detection and suppression.

You can modify the duplicate MAC address detection settings on the switches by configuring the detection window for identifying duplicate MAC address and the number of MAC address moves detected within the detection window before duplicate MAC detection is triggered and the MAC address is suppressed. In addition, you can also configure an optional recovery time that the switches wait before the duplicate MAC address is automatically unsuppressed.

To configure duplicate MAC detection parameters, use the **detection-window**, **detection-threshold**, and **auto-recovery-time** statements at the **[edit routing instance *routing-instance-name* protocols evpn duplicate-mac-detection]** hierarchy level.

To clear duplicate MAC suppression manually, use the **clear evpn duplicate-mac-suppression** command.

[See [Overview of MAC Mobility](#).]

Interfaces and Chassis

- **Generic routing encapsulation (GRE) support (QFX10002-60C switches)**— Starting with Junos OS Release 18.1R1, you can use GRE tunneling services to encapsulate any network layer protocol over an IP network. Acting as a tunnel source router, the switch encapsulates a payload packet that is to be transported through a tunnel to a destination network. The switch first adds a GRE header and then adds an outer IP header that is used to route the packet. When it receives the packet, a switch performing the role of a tunnel remote router extracts the tunneled packet and forwards the packet to the destination network. GRE tunnels can be used to connect noncontiguous networks and to provide options for networks that contain protocols with limited hop counts.
- **Support for private VLANs and support for IRB in P-VLAN (QFX5210 switches)**— Starting with Junos OS Release 18.1R1, QFX5210 switches support private VLANs. VLANs limit broadcasts to specified users. Private VLANs (P-VLANs) take this concept a step further by splitting the broadcast domain into multiple isolated broadcast subdomains and essentially putting secondary VLANs inside a primary VLAN. P-VLANs restrict traffic flows through their member switch ports (called “private ports”) so that these ports communicate only with a specified uplink trunk port or with specified ports within the same VLAN.

The uplink trunk port is usually connected to a router, firewall, server, or provider network. Each P-VLAN typically contains many private ports that communicate only with a single uplink, thereby preventing the ports from communicating with each other.

Just like regular VLANs, P-VLANs are isolated on Layer 2 and require that a Layer 3 device be used to route traffic among them. P-VLANs are useful for restricting the flow of broadcast and unknown unicast traffic and for limiting the communication between known hosts. Service providers use P-VLANs to keep their customers isolated from one another.

[See [Understanding Private VLANs](#).]

Also starting with Junos OS Release 18.1R1, you can configure an integrated routing and bridging (IRB) interface in a private VLAN (P-VLAN) so that devices within community VLANs and isolated VLANs can communicate with each other and with devices outside the P-VLAN at Layer 3 without requiring you to install a router.

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

- **FEC support for 25-gigabit and 50-gigabit channel speeds (QFX5210 switches)**—Starting with Junos OS Release 18.1R1, you can configure forward error correction (FEC) clauses CL74 and CL91 on QFX5210 switches. FEC CL91 can be configured on 100-gigabit interfaces and FEC CL74 can be configured on 25-gigabit and 50-gigabit interfaces. Because the FEC clauses are applied by default on these interfaces, you must disable the FEC clauses if you do not want to apply them.

- To disable the FEC mode:

```
[edit]
set interfaces interface-name gigether-options fec none
```

- To reenable the FEC mode:

```
[edit]
set interfaces interface-name gigether-options fec (fec74|fec91)
```

or

```
[edit]
delete interfaces interface-name gigether-options fec none
```

- 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.

[See [FEC](#).]

- **Resilient hashing support for equal cost multipath routes (QFX5210 switches)**—Starting with Junos OS Release 18.1R1, resilient hashing is now supported by equal cost multipath (ECMP) sets.

NOTE: Resilient hashing is not supported on link aggregations groups (LAGs).

[See [Understanding the Use of Resilient Hashing to Minimize Flow Remapping in Trunk Groups](#).]

- **Multichassis link aggregation groups (MC-LAG) (QFX5210 switches)**—Starting with Junos OS Release 18.1R1, MC-LAG enables a client device to form a logical LAG interface using two switches. MC-LAG provides redundancy and load balancing between the two switches, multihoming support, and a loop-free Layer 2 network without running STP.

On one end of an MC-LAG is an MC-LAG client that has one or more physical links in a LAG. This client does not need to detect the MC-LAG. On the other side of the MC-LAG are two MC-LAG QFX10008 switches. Each of these switches has one or more physical links connected to a single client. The switches coordinate with each other to ensure that data traffic is forwarded properly.

[See [Multichassis Link Aggregation Features, Terms, and Best Practices](#).]

- **Auto-channelization of interfaces (QFX5210 switch)**—Starting in Junos OS Release 18.1R1, 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 QFX5210, 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.
- **Channelization support (QFX10002-60C switches)**—Starting with Junos OS Release 18.1R1, you can use channelization functionality to subdivide a larger flexible optical interface into sub-interfaces or channels. The QFX10002-60C switch has 12 ASIC circuits (PE) as a part of a Packet Forwarding Engine, and each PE switch has 5 ports (one standalone MAC port and 4 channelized MAC ports). The standalone MAC ports cannot be channelized. The QFX10002-60C switch allows you to channelize 48 ports out of available 60 ports.

By default, the ports come up in a mode that does not support channelization. If you channelize a port in a PE switch for the first time, it would result in FPC reboot. But if you channelize another port in the same PE switch, the FPC will not be rebooted. If you channelize a port in a different PE switch, the FPC will be rebooted.

To enable channelization on an interface:

```
[edit chassis fpc fpc-slot pic pic-slot]
```

```
user@switch# set port port-number channel-speed speed
```

[See [Channelizing Interfaces](#).]

- **Dynamic port swap from 40G to 100G without restarting the Packet Forwarding Engine (QFX5110 switches)**—Starting in Junos OS Release 18.1R1, you can configure different system modes to achieve varying levels of port density on QFX5110-32Q switches without restarting the Packet Forwarding Engine. The QFX5110-32Q switch has fixed 32 front panel network ports. Four 100G ports can either function as 32x40G or 20x40G – 4x100G. You can combine the port configurations supported into default mode or non-oversubscribed mode. The **dcufe** restart is triggered with the mode change.
- **Support for 128k vmembers and 96k Address Resolution Protocol (ARP) and Neighbor Discovery (ND) entries when using enhanced convergence in multichassis link aggregation groups (MC-LAG) (QFX10000 switches)**—Starting with Junos OS Release 18.1R1, the number of vmembers has increased to 128k, and the number of ARP and ND entries has increased to 96k. This increased scale is supported only when you enable the **enhanced-convergence** statement. Enhanced convergence improves Layer 2 and Layer 3 convergence time during multichassis aggregated Ethernet (MC-AE) link failures and restoration scenarios.

If you have configured an IRB interface over an MC-AE interface that has enhanced convergence enabled, then you must configure enhanced convergence on the IRB interface as well. Enhanced convergence must be enabled for both Layer 2 and Layer 3 interfaces.

To configure enhanced convergence, enable the **enhanced-convergence** statement at the **[edit interfaces ae *unit-number* aggregated-ether-options mc-ae]** at the Junos OS CLI hierarchy.

To configure enhanced convergence on an IRB interface, enable the **enhanced-convergence** statement at the **[edit interfaces irb unit *unit-number*]** at the Junos OS CLI hierarchy.

[See [Multichassis Link Aggregation Features, Terms, and Best Practices](#).]

- **Support for additional 10G data ports (QFX5210 switches)**—Starting in Junos OS Release 18.1R1, QFX5210 switches support two additional 10G data ports. You can use the two additional data ports as revenue ports.
- **FEC support for 100-gigabit port speeds (QFX10002, QFX10008, and QFX10016 Switches)**—Starting with Junos OS Release 18.1R1, you can configure forward error correction (FEC) clause CL91 on QFX10000 series switches. FEC CL91 can be configured on 100-gigabit interfaces. FEC CL91 clause is applied by default on these interfaces. If you do not want to apply the FEC CL91 clause, you can disable it.

- To disable the FEC mode:

```
[edit]
set interfaces interface-name together-options fec none
```

- To reenab the FEC mode:

```
[edit]
set interfaces interface-name gigether-options fec (fec74|fec91)
```

or

```
[edit]
delete interfaces interface-name gigether-options fec none
```

- 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.

[See [FEC](#).]

- **Support for Protocol Independent Multicast (PIM) Dual Designated Router Mode (QFX10002, QFX10008, and QFX10016 switches)**—Starting in Junos OS Release 18.1R1, you can enable PIM dual designated router mode for a pair of Multichassis Link Aggregation Group (MC-LAG) peers managing VLAN multicast traffic and Layer 3 multicast traffic over IRB interfaces.

PIM dual designated router mode sets up one device in a pair of MC-LAG peers as a primary designated router (DR), and the other device as a standby or backup DR for redundancy in managing multicast packet forwarding. Both devices join the multicast forwarding tree and receive multicast traffic. If the primary device fails, the standby device quickly takes over forwarding multicast packets with minimal traffic disruption.

- **Link Aggregation Control Protocol (LACP) force-up enhancements (QFX5210 switches)**—Starting in Junos OS Release 18.1R1, if an aggregated Ethernet interface (AE) on a switch has multiple member links and one member link in that AE is in the force-up state with its peer's LACP down, and then if LACP comes up partially—that is, if LACP is established with a non-force-up member link—force-up is disabled on the member link on which force-up has been set, and that member link is ready for connection establishment through LACP. Force-up is eligible only if the server-side interface has LACP issues.
- **Channelization support (QFX10002-60C switches)**—Starting with Junos OS Release 18.1R1, you can use channelization functionality to subdivide a larger flexible optical interface into sub-interfaces or channels. The QFX10002-60C switch has 12 ASIC circuits (PE) as a part of a Packet Forwarding Engine, and each PE switch has 5 ports (one standalone MAC port and 4 channelized MAC ports). The standalone MAC ports cannot be channelized. The QFX10002-60C switch allows you to channelize 48 ports out of available 60 ports.

By default, the ports come up in a mode that does not support channelization. If you channelize a port in a PE switch for the first time, it would result in FPC reboot. But if you channelize another port in the

same PE switch, the FPC will not be rebooted. If you channelize a port in a different PE switch, the FPC will be rebooted.

To enable channelization on an interface:

```
[edit chassis fpc fpc-slot pic pic-slot]
user@switch# set port port-number channel-speed speed
```

[See [Channelizing Interfaces](#).]

- **Generic routing encapsulation (GRE) support (QFX10002-60C switches)**—Starting with Junos OS Release 18.1R1, you can use GRE tunneling services to encapsulate any network layer protocol over an IP network. Acting as a tunnel source router, the switch encapsulates a payload packet that is to be transported through a tunnel to a destination network. The switch first adds a GRE header and then adds an outer IP header that is used to route the packet. When it receives the packet, a switch performing the role of a tunnel remote router extracts the tunneled packet and forwards the packet to the destination network. GRE tunnels can be used to connect noncontiguous networks and to provide options for networks that contain protocols with limited hop counts.
- **Channelizing Ethernet interfaces (QFX5200 switches)**—Starting with Junos OS Release 18.1R1, you can channelize the 100-Gigabit Ethernet interfaces to two independent 50-Gigabit Ethernet. The default 100-Gigabit Ethernet interfaces can also be configured as 40-Gigabit Ethernet interfaces, and in this configuration can either operate as dedicated 40-Gigabit Ethernet interfaces or can be channelized to four independent 10-Gigabit Ethernet interfaces using breakout cables.

There are a total of 54 physical ports on the QFX5200 switch. Ports 0 - 47 can be used as 25-Gigabit Ethernet interfaces. Ports 48 - 53 can be used as either 40-Gigabit Ethernet or 100-Gigabit Ethernet interfaces. You choose the speed by plugging in the appropriate transceiver. They can also be channelized to 10G, 40G, or 100G.

[See [Channelizing Interfaces on QFX Switches](#).]

- **Channelizing Ethernet Interfaces (QFX5210 switches)**—Starting with Junos OS Release 18.1R1, you can channelize the 100-Gigabit Ethernet interfaces to two independent 50-Gigabit Ethernet or to four independent 25-Gigabit Ethernet interfaces. The default 100-Gigabit Ethernet interfaces can also be configured as 40-Gigabit Ethernet interfaces, and in this configuration can either operate as dedicated 40-Gigabit Ethernet interfaces or can be channelized to four independent 10-Gigabit Ethernet interfaces using breakout cables.

There are a total of 64 physical ports on the QFX5210 switch. Any port can be used as either 100-Gigabit Ethernet or 40-Gigabit Ethernet interfaces. You choose the speed by plugging in the appropriate transceiver. They can also be channelized to 50G, 25G or 10G.

[See [Channelizing Interfaces on QFX Switches](#).]

IPv4

- **Generic routing encapsulation (GRE) support (QFX5200 and QFX5210 switches)**—Starting in Junos OS Release 18.1R1, you can use GRE tunneling services to encapsulate any network layer protocol over an IP network. Acting as a tunnel source router, the switch encapsulates a payload packet that is to be transported through a tunnel to a destination network. The switch first adds a GRE header and then adds an outer IP header that is used to route the packet. When it receives the packet, a switch performing the role of a tunnel remote router extracts the tunneled packet and forwards the packet to the destination network. GRE tunnels can be used to connect noncontiguous networks and to provide options for networks that contain protocols with limited hop counts.
- **Layer 2, Layer 3, multicast, IPv4, IPv6, and hierarchical ECMP support (QFX5210-64C switches)**—Starting in Junos OS Release 18.1R1, the feature set supporting the QFX5200 switch for Junos OS Release 17.3 DCB also supports the QFX5210-64C switch.

IPv6

- **Layer 2, Layer 3, multicast, IPv4, IPv6, and hierarchical ECMP support (QFX5210-64C switches)**—Starting in Junos OS Release 18.1R1, the feature set supporting the QFX5200 switch for Junos OS Release 17.3 DCB also supports the QFX5210-64C switch.

Junos OS XML API and Scripting

- **SLAX and Python scripts now can be sourced over the non-default VRF management instance (QFX Series)**—Starting in Junos OS Release 18.1R1, configuration of commit, event, JET, op, and SNMP scripts is upgraded to support the non-default management routing instance `mgmt_junos` as an option when specifying the source URL for refreshing or downloading SLAX and Python scripts.

[See [Using an Alternate Source Location for a Script](#) or [Configuring and Using a Master Source Location for a Script](#).]

Layer 2 Features

- **Layer 2 features (QFX5210 switches)**—Starting with Junos OS Release 18.1R1, the following Layer 2 features are supported:
 - **VLAN support**
VLANs enable you to divide one physical broadcast domain into multiple virtual domains.
 - **Link Layer Discovery Protocol (LLDP) support**
LLDP enables a switch to advertise its identity and capabilities on a LAN, as well as receive information about other network devices.
 - **Q-in-Q tunneling support**
This feature enables service providers on Ethernet access networks to extend a Layer 2 Ethernet connection between two customer sites.
 - **Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP) support**

These protocols enable a switch to advertise its identity and capabilities on a LAN and receive information about other network devices.

[See [Ethernet Switching User Guide](#).]

- **Layer 2, Layer 3, multicast, IPv4, IPv6, and hierarchical ECMP support (QFX5210-64C switches)**—Starting in Junos OS Release 18.1R1, the feature set supporting the QFX5200 switch for Junos OS Release 17.3 DCB also supports the QFX5210-64C switch.

Layer 3 Features

- **Layer 2, Layer 3, multicast, IPv4, IPv6, and hierarchical ECMP support (QFX5210-64C switches)**—Starting in Junos OS Release 18.1R1, the feature set supporting the QFX5200 switch for Junos OS Release 17.3 DCB also supports the QFX5210-64C switch.

Management

- **Support for the Junos Telemetry Interface (QFX5100 switches)**—Starting with Junos OS Release 18.1R1, you can provision sensors through the Junos Telemetry Interface to export telemetry data for various network elements without involving polling. On QFX5100 switches, only gRPC streaming of statistics is supported. UDP streaming is not supported.

To provision the sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. For streaming through UDP, all parameters are configured at the **[edit services analytics]** hierarchy level.

For resource names and OpenConfig paths for these sensors, see *Guidelines for gRPC Sensors (Junos Telemetry Interface)*

The following sensors are supported:

- Chassis components
- Aggregated Ethernet interfaces configured with the Link Aggregation Control Protocol
- Network Discovery Protocol table state

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

- **ARP and NDP telemetry support for Junos Telemetry Interface (JTI) (QFX5110)**—Starting with Junos OS Release 18.1R1, you can export Address Resolution Protocol (ARP) and Neighbor Discovery Protocol (NDP) statistics through the Junos Telemetry Interface for QFX5110 switches. Sensor support for ARP and NDP statistics is at the same level of support as for QFX10000 and QFX5200 switches in Junos OS Release 17.2R1.

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

To export telemetry data from Juniper equipment to an external collector, both Junos Telemetry Interface (JTI) and gRPC must be configured.

For resource names and OpenConfig paths for these sensors, see [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#).

MPLS

- **Support for equal-cost multipath routing on MPLS label-switching routers (QFX5210 switches)**—Starting in Junos OS Release 18.1R1, you can configure equal cost multipath (ECMP) routing on MPLS label-switched routers (LSRs). ECMP is a Layer 3 mechanism for load-balancing traffic to a destination over multiple equal-cost next hops. When a link goes down, ECMP uses fast reroute protection to shift packet forwarding to use operational links, thereby decreasing packet loss.

This feature was previously supported in an "X" release of Junos OS.

[See [Understanding ECMP Flow-Based Forwarding](#).]

- **MPLS support (QFX5210 switches)**—Starting in Junos OS Release 18.1R1, MPLS is supported on the QFX5210 switch. MPLS provides both label edge routers (LER) and label switch routers (LSR) and provides the following capabilities:
 - Support for both MPLS major protocols, LDP and RSVP
 - IS-IS interior gateway protocol (IGP) traffic engineering
 - Class of service (CoS)
 - Object access method, including ping, traceroute, and Bidirectional Forwarding Detection (BFD)
 - Fast reroute (FRR), a component of MPLS local protection. (Both one-to-one local protection and many-to-one local protection are supported.)
 - Loop-free alternate (LFA)
 - 6 PE devices
 - Layer 3 VPNs for both IPv4 and IPv6
 - LDP tunneling over RSVP

This feature was previously supported in an "X" release of Junos OS.

[See [MPLS Overview for Switches](#).]

Multicast

- **Multicast-only fast reroute (MoFRR) (QFX10002, QFX10008, and QFX10016 switches)**—Starting in Junos OS Release 18.1R1, QFX10002, QFX10008, and QFX10016 switches support MoFRR, which minimizes multicast packet loss in PIM domains when there are link failures. With MoFRR enabled, the switch maintains both a primary and a backup multicast packet stream toward the multicast source,

accepting traffic received on the primary path and dropping traffic received on the backup path. Upon primary path failure, the backup path becomes the primary path and quickly takes over forwarding the multicast traffic. If alternative paths are available, a new backup path is created. When enabling MoFRR, you can optionally configure a policy for the (S,G) entries to which MoFRR should apply; otherwise, MoFRR applies to all multicast (S,G) streams.

[See [Understanding Multicast-Only Fast Reroute on Switches](#).]

- **Layer 2, Layer 3, multicast, IPv4, IPv6, and hierarchical ECMP support (QFX5210-64C switches)**—Starting in Junos OS Release 18.1R1, the feature set supporting the QFX5200 switch for Junos OS Release 17.3 DCB also supports the QFX5210-64C switch.

Network Management and Monitoring

- **Support for sFlow, port mirroring, and port mirroring to an IP address (QFX5210 switches)**—Starting in Junos OS Release 18.1 R1 the QFX5210 switch supports sFlow technology. sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring randomly samples network packets and sends the samples to a monitoring station called a collector. You can configure sFlow monitoring on the switch to continuously monitor traffic at wire speed on all interfaces simultaneously. sFlow monitoring also collects samples of network packets, providing you with visibility into network traffic information. You configure sFlow monitoring at the **edit protocols sflow** hierarchy level. sFlow operational commands include **show sflow** and **clear sflow collector statistics**. This feature was previously supported in an "X" release of Junos OS.

[See [Understanding How to Use sFlow Technology for Network Monitoring on a Switch](#).]

Also starting in Junos OS Release 18.1R1, you can use port mirroring on QFX5210 switches to copy packets entering or exiting a port or entering a VLAN and send the copies to a local interface for local monitoring or to a VLAN for remote monitoring. 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, and correlating events. This feature was previously supported in an "X" release of Junos OS.

[See [Understanding Port Mirroring](#).]

Finally, also starting in Junos OS Release 18.1R1, you can send mirrored packets to an IP address over a Layer 3 network (for example, if there is no Layer 2 connectivity to the analyzer device). This feature also enables you to apply an IEEE-1588 timestamp to the mirrored packets. This feature was previously supported in an "X" release of Junos OS.

[See [Understanding Port Mirroring](#).]

Port Security

- **MACsec license enforcement (EX3400, EX4300, EX4600, EX9200, QFX5100 switches and Junos Fusion Enterprise)**—Starting in Junos OS Release 18.1R1, Media Access Control Security (MACsec) requires the installation of a MACsec feature license. If the MACsec license is not installed, MACsec functionality cannot be activated. You add the MACsec license using the **request system license add** command.

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

Routing Protocols

- **Support for BGP multipath at global level (QFX Series)**—Starting with Junos OS Release 18.1 R1, BGP multipath is available at the global level. In earlier Junos OS releases BGP multipath is supported only at the group level. A new configuration option **disable** is available at the **[edit protocols bgp group]** hierarchy level to disable BGP multipath at the group level. This allows you to configure BGP multipath globally and disable it for specific groups according to your network requirements.

Security

- **Distributed denial-of-service (DDoS) protection (QFX5210 switches)**—Starting with Junos OS Release 18.1R1, you can use DDoS protection to enable the switch to continue functioning while under a DDoS attack.

[See [Understanding Distributed Denial-of-Service Protection on QFX Series Switches.](#)]

- **Support for firewall filters (QFX5210)**—Starting in Junos OS Release 18.1R1, you can define firewall filters on the switch that defines 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 configure firewall filters at the `[edit firewall]` hierarchy level.

This feature was previously supported in an “X” release of Junos OS.

[See [Overview of Firewall Filters.](#)]

- **Storm control support (QFX5210 switches)**—Starting in Junos OS Release 18.1R1, you can monitor traffic levels and take a specified action when a defined traffic level (called the storm control level) is exceeded, preventing packets from proliferating and degrading service. You can configure the switch to drop broadcast and unknown unicast packets, shut down interfaces, or temporarily disable interfaces when a traffic storm occurs.

This feature was previously supported in an “X” release of Junos OS.

[See [Understanding Storm Control.](#)]

- **Support for policers (QFX5210 switches)**—Starting in Junos OS Release 18.1R1, you can use policers to apply limits to traffic flow and to set consequences for packets that exceed those limits. A switch polices traffic by limiting the input or output transmission rate of a class of traffic according to user-defined criteria. Policing (or rate-limiting) traffic allows you to control the maximum rate of traffic sent or received on an interface and to provide multiple priority levels or classes of service.

This feature was previously supported in an “X” release of Junos OS.

[See [Overview of Policers.](#)]

Software-Defined Networking

- **Layer 2 VXLAN gateway (QFX5210 switches)**—Virtual Extensible LAN (VXLAN) is an overlay technology that allows you to stretch Layer 2 connections over an intervening Layer 3 network by encapsulating (tunneling) Ethernet frames in a VXLAN packet that includes IP addresses. You can use VXLAN tunnels to enable migration of virtual machines between servers that exist in separate Layer 2 domains by tunneling the traffic through Layer 3 networks. This functionality allows you to dynamically allocate resources within or between data centers without being constrained by Layer 2 boundaries or being forced to create large or geographically stretched Layer 2 domains.

Starting with Junos OS Release 18.1R1, you can manually create VXLANs on QFX5210 switches instead of using a controller such as a VMware NSX for vSphere or Juniper Networks Contrail controller. If you use this approach, you must also configure Protocol Independent Multicast (PIM) on the VTEPs so that they can create VXLAN tunnels between themselves.

[See [Understanding VXLANs.](#)]

- **OVSDB-VXLAN support with VMware NSX for vSphere (QFX5210 switches)**—Starting with Junos OS Release 18.1R1, the Open vSwitch Database (OVSDB) management protocol provides a means through which an NSX for vSphere controller can communicate with QFX5210 switches and provision them as Layer 2 Virtual Extensible LAN (VXLAN) gateways. In an environment in which NSX for vSphere 6.3.5 or later is deployed, an NSX for vSphere controller and these switches can exchange control and statistical information, thereby enabling virtual machine (VM) traffic from entities in a virtualized network to be forwarded to entities in a physical network and vice versa.

[See [Understanding the OVSDB Protocol Running on Juniper Networks Devices.](#)]

- **OVSDB-VXLAN support with VMware NSX for vSphere (QFX5110 and QFX5200 switches)**—Starting with Junos OS Release 18.1R1, the Open vSwitch Database (OVSDB) management protocol provides a means through which an NSX for vSphere controller can communicate with QFX5110 and QFX5200 switches and provision them as Layer 2 Virtual Extensible LAN (VXLAN) gateways. In an environment in which NSX for vSphere 6.3.5 or later is deployed, an NSX for vSphere controller and these switches can exchange control and statistical information, thereby enabling virtual machine (VM) traffic from entities in a virtualized network to be forwarded to entities in a physical network and vice versa.

[See [Understanding the OVSDB Protocol Running on Juniper Networks Devices.](#)]

Software Installation and Upgrade

- **ZTP support (QFX10002-60C switch)**—Starting with Junos OS Release 18.1R1, ZTP, automates the provisioning of the device configuration and software image with minimal manual intervention, and is supported on QFX10002-60C 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.](#)]

Storage and Fibre Channel

- **Support for FIP snooping and DCBX (QFX5210)**—Starting in Junos OS Release 18.1R1, QFX5210 switches support FCoE Initialization Protocol (FIP) snooping and Data Center Bridging Capability Exchange protocol (DCBX), which are technologies that help enable transporting converged Ethernet traffic. FIP snooping filters prevent FCoE devices from gaining unauthorized access to a Fibre Channel (FC) storage device or another FCoE device. DCBX discovers the data center bridging (DCB) capabilities of connected peers, and advertises the capabilities of applications on interfaces by exchanging information in the form of application type, length, and value elements (TLVs).

[See [Storage User Guide](#) and [Traffic Management User Guide for the QFX Series and EX4600 Switches.](#)]

- **Support for Converged Enhanced Ethernet (CEE) features (QFX5210)**—Starting in Junos OS Release 18.1R1, QFX5210 switches support the following data center bridging (DCB) traffic management features for transporting CEE traffic:

- Priority-based flow control (PFC) for traffic prioritization and managing link bandwidth for lossless traffic
- Buffer space management to prevent dropped traffic with PFC
- Congestion notification for managing link bandwidth, including Explicit Congestion Notification (ECN) and Data Center Quantized Congestion Notification (DCQCN)
- Data Center Bridging Capabilities Exchange protocol (DCBX)

CEE enables traffic differentiation at the link layer and sharing of links for both Ethernet and FCoE traffic.

[See [Traffic Management User Guide for the QFX Series and EX4600 Switches](#).]

System Management

- **Integrated software feature licenses (QFX5210 switches)**—Starting with Junos OS Release 18.1R1, the standard QFX Series premium feature license for BGP, Intermediate System-to-Intermediate System (IS-IS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDb) software license and the standard QFX Series advanced feature license for BGP, Intermediate System-to-Intermediate System (IS-IS), MPLS, and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDb) license are supported.

[See [Software Features That Require Licenses on the QFX Series](#).]

- **Support for the Precision Time Protocol (PTP) G.8275.2 enhanced profile (QFX5110-48S-4C switches)**—Starting in Junos OS Release 18.1R1, you can enable the G.8275.2 enhanced profile to support telecom applications that require accurate phase and time synchronization for phase alignment and time of day synchronization over a wide area network. This profile supports PTP over IPv4 unicast, ordinary and boundary clocks, and unicast negotiation.

To configure the G.8275.2 enhanced profile, enable the **g.8275.2.enh** statement at the **[edit protocols ptp profile-type]** Junos OS CLI hierarchy.

[See [Understanding the PTP G.8275.2 Enhanced Profile \(Telecom Profile\)](#).]

- **Support for request vmhost and show vmhost commands (QFX10002-60C switches)**—Starting in Junos OS Release 18.1R1, many of the **request system** and **show system** commands have been replaced with **request vmhost** and **show vmhost** commands.

Here is a list of the vmhost commands that are now supported:

- request vmhost cleanup
- request vmhost file-copy
- request vmhost halt
- request vmhost hard-disk-test
- request vmhost power-off
- request vmhost power-on

- request vmhost reboot
- request vmhost snapshot
- request vmhost software add
- request vmhost software rollback
- request vmhost zeroize
- show vmhost bridge
- show vmhost crash
- show vmhost hard-disk-test
- show vmhost hardware
- show vmhost information
- show vmhost logs
- show vmhost management-if
- show vmhost netstat
- show vmhost processes
- show vmhost resource-usage
- show vmhost snapshot
- show vmhost status
- show vmhost uptime
- show vmhost version

[See [VM Host Operations and Management](#) for more information.]

SEE ALSO

[Changes in Behavior and Syntax](#) | 227

[Known Behavior](#) | 229

[Known Issues](#) | 234

[Resolved Issues](#) | 240

[Documentation Updates](#) | 248

[Migration, Upgrade, and Downgrade Instructions](#) | 249

[Product Compatibility](#) | 263

Changes in Behavior and Syntax

IN THIS SECTION

- [Interfaces and Chassis | 227](#)
- [Management | 227](#)
- [Network Management and Monitoring | 228](#)
- [Network Operations and Troubleshooting Automation | 228](#)
- [Routing Policy and Firewall Filters | 229](#)

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 18.1R2 for the QFX Series.

Interfaces and Chassis

- **Modified output of show-ptp-clock command (QFX Series switches)**—Starting in Junos OS Release 18.1R1, the output of the **show-ptp-clock** command is modified to display the value of the **GMC Class** field as **248** for a PTP boundary clock when the lock state of the clock is **Acquiring**.

Management

- **Enhancement to LSP statistics sensor for Junos Telemetry Interface (MX Series, PTX Series, QFX10000 switches, and EX9200 switches)**—Starting with Junos OS 18.1R1, the telemetry data exported for the LSP statistics sensor no longer includes the phrase **and source 0.0.0.0** after the LSP name in the value string for the prefix key. This change reduces the payload size of data exported. The following is an example of the new format:

```
str_value: /mpls/lsp/constrained-path/tunnels/tunnel[name='LSP-4-3']/state/
counters[name='c-27810']/
```

- **Enhancement to NPU memory sensors for Junos Telemetry Interface (QFX5110, QFX5200, and QFX10000 switches)**—Starting with Junos OS Release 18.1R1, the format of telemetry data exported through gRPC for NPU memory and memory utilization implements prefix compression. This change reduces the payload size of data exported. The following example shows the new format:

```
key: __prefix__
str_value: /components/component[name='FPC0:NPU0']/properties/property
key: [name='mem-util-edmem-size']/value
uint_value: 12345
```

Telemetry data is exported in key-value pairs. Previously, the data exported included the component and property names in a single key string.

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

Network Management and Monitoring

- **SNMP syslog messages changed (QFX Series)**—In Junos OS Release 18.1R1, 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](#).]

Network Operations and Troubleshooting Automation

- **JET - Correction to escaped characters notification events** (QFX Series data center switches)—Per RFC7159, certain characters must be escaped. Data returned from JET notification subscriptions contained escaped characters that were not required. This has been corrected to comply with RFC7159.
- **respawn-on-normal-exit** option added to [**edit system extensions extension-service application file <application-name>**] hierarchy (QFX Series Data Center Switches)—This option helps to ensure that daemonized Juniper Extension Toolkit (JET) applications that exit normally will restart without user intervention. Daemonized JET applications that exit unexpectedly will still restart without user intervention. This is the default behavior.

Routing Policy and Firewall Filters

- **Support for configuring the GTP-TEID field for GTP traffic (QFX5000 line of switches)**—Starting in Junos OS Release 17.3R3 and 18.1R2, 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](#).]

SEE ALSO

New and Changed Features 208
Known Behavior 229
Known Issues 234
Resolved Issues 240
Documentation Updates 248
Migration, Upgrade, and Downgrade Instructions 249
Product Compatibility 263

Known Behavior

IN THIS SECTION

- [EVPN | 230](#)
- [Interfaces and Chassis | 230](#)
- [Junos Fusion Provider Edge | 230](#)
- [Layer 2 Features | 231](#)
- [Multicast | 231](#)

- Platform and Infrastructure | 231
- Routing Protocols | 233
- Services Applications | 234
- Storage and Fibre Channel | 234

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.1R2 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.

EVPN

- 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](#)
- EVPN-VXLAN implementations support up to 100 EVPN VLAN-based routing instances. Above 100 instances, MAC learning might behave incorrectly. [PR1287644](#)

Interfaces and Chassis

- Because the link speed command cannot be hidden, configuring or committing the same should not result in the intended functionality. Otherwise, MC-LAG peer states will get impacted. [PR1329030](#)
- Force UP on LAG/MC-LAG feature is not supported on QFX10000 platform. [PR1332475](#)
- Supported ARP scale is 48,000 over MC-LAG interfaces. [PR1334321](#)

Junos Fusion Provider Edge

- Configuration synchronization is not triggered when you issue the rollback command on the local aggregation device (AD). [PR1298747](#)
- Since EVPN GR is not supported, restart of rpd will result in considerable traffic loss for EVPN traffic. The traffic should restore eventually once convergence is complete. [PR1353742](#)

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 a VXLAN-enabled IRB interface is configured in the same routing instance as that of 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 core files would be generated and all the interfaces would go down. dc-pfe cores would be continuously generated until the configuration is corrected. [PR1261824](#)
- LAG-based resilient hashing is not supported on QFX5200 and QFX5210 switches. ECMP-based resilient hashing is supported on those switches. [PR1321505](#)
- QFX5210-64C: Resilient hashing is not supported for LAG interfaces. [PR1325499](#)
- Packet statistics are not supported for logical child members of aggregated Ethernet (AE) interface. [PR1335454](#)
- Supported global Vmember scale is 64,000 when created over AE interfaces [PR1337569](#)

Multicast

- To use IGMP snooping on QFX5110 switches in an EVPN-VXLAN multihoming environment, you must enable IGMP snooping on all VLANs associated with any configured VXLANs. You cannot selectively enable IGMP snooping only on those VLANs that might have interested listeners, because all the VXLANs share virtual tunnel endpoints (VTEPs) between the same multihoming peers and must have the same settings. [PR1407557](#)

Platform and Infrastructure

- On the QFX10000-12C-DWDM coherent line card, the link might flap when MACsec is enabled on Ethernet interfaces. [PR1253703](#)
- ERPS convergence takes time after GRES switchover and hence traffic loss is observed for a brief period. [PR1290161](#)
- On QFX Series, the physical interface(IFD) and the logical interface (IFL) go down when traffic exceeds rate-limit. Storm control is supported only on interfaces configured in family Ethernet-switching. Moreover, in this family, only one IFL per IFD is supported. Due to this, bringing down the IFD is acceptable. Flexible VLAN tagging is not supported on the interfaces enabled for storm control. [PR1295523](#)
- On QFX10000 line platforms, with a high scale of 4000 VNIs or 200,000 MAC addresses, 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 such as global MAC count and underlying MPLS LSPs might increase system load. [PR1296089](#)

- em1 does not show correct speed when its other end is connected to 10m/100m ports. [PR1303902](#)
- 18.1-20171108_dev_common_tvp.0 And one more main requirement with CoS on FC interface is , FC interface should be brought down before applying any COS configuration. So we need to admin down the interface, apply the cos configuration and admin up the interface. This is required due to HW (BCM) limitation. [PR1320425](#)
- On a 100G DAC/copper cable connected between QFX5210-64C and QFX10000 devices, links might not come up reliably. The rest of the 100G Optics/AOC, 40G Optics/DAC/Copper work well when connected between QFX5210-64C and QFX10000 devices. [PR1324600](#)
- Configuration of **mac-table-size** under VLAN **switch-options** is not supported for QFX10002-60C. [PR1325315](#)
- QFX5210-64C : Irrespective of the physical interface speed, speed displayed for Gr-interface is always 800 mbps. [PR1325695](#)
- The **mac-learning-limit** option is not supported under vlan switch-options for QFX10002-60C platform [PR1325752](#)
- Since for a given logical interface, both IPv4 and IPv6 use the same VLAN, statistics will count both IPv4 and IPv6 together. There is no way to separately count them. Hence, "IPv6 transit statistics" is always 0. However, the total transit statistics (IPv4 + IPv6) will be displayed under "Transit statistics". [PR1327811](#)
- Need to increase global-mac-table-aging-time and global-mac-ip-table-aging-time settings on Junos Fusion Provider Edge ADs: **set protocols l2-learning global-mac-table-aging-time 900 set protocols l2-learning global-mac-ip-table-aging-time 720**[PR1328929](#)
- Configuring IRB physical interface (IFD) static MAC address takes effect only if the logical interface (IFL) level static configuration works. [PR1329032](#)
- Because the scaling numbers for flex counters in Broadcom are less than the number of maximum multicast routes that can be installed in hardware and also the flex counters are shared among different entities such as VFI, VRF, VFP, L3IIF, SOURCE_VP, MPLS_ENTRY, VLAN_XLATE,PORT_TABLE,L3_ENTRY_IPV4_MULTICAST,L3_ENTRY_IPV6_MULTICAST,L3_DEFIP, creation of counter will fail after the scale limit is reached (70000 and it shared). [PR1330473](#)
- The use of **flexible-vlan-tagging** with two VLAN tags is not supported on Layer 3 logical interfaces on QFX5110-48S and QFX5200 switches. [PR1330510](#)
- The **rt_pfe_veto** related error messages might be seen when a large number of routes are learned and downloaded to FIB. The messages indicate how slowly the Packet Forward Engines installs the routes in the hardware and do not have any functionality impact. [PR1333553](#)
- A few error messages related to function **rt_mesh_group_add_check()** will be seen during reboot and are harmless. [PR1335363](#)
- Analyzer is not supported on QFX10002-60C. [PR1335970](#)

- Inline and distributed BFD is not supported for IRB interfaces. Please configure BFD timers according to the guidelines for centralized mode. The problem is more pronounced in IS-IS because more packets (L1 and L2) are needed to maintain the sessions. [PR1339127](#)
- On QFX5110-48S, PTP Delay-Req packets might be generated at less than 128 pps when the delay-request interval is configured as -7. [PR1339775](#)
- On QFX5100 platform multihop BFD session(s) might flap after disruptive trigger in topology with aggressive BFD timeout less than 1 second. Examples of disruptive triggers include restarting routing and rebooting the router. [PR1340469](#)
- In an IP CLOS topology, when a spine or leaf is rebooted, you might see around 100 seconds of traffic loss. The reason for this is that Junos OS will start advertising routes before Packet Forwarding Engine route programming is completed, which can cause traffic loss. This is mainly a design tradeoff. If you wait for Packet Forwarding Engine programming to complete, then route convergence will suffer. [PR1341398](#)
- In scaled VRRP scenario with 1000 groups, it takes around 17 seconds for all traffic to converge onto the backup node. [PR1341811](#)
- On switching platforms LACP AE minimum-link with sync-reset enabled feature is not supported on an aggregated interface where MicroBFD is enabled. [PR1342657](#)
- On upgrading QFX10002 from Junos OS Release 15.1X53-D66 to Release 18.1R1, some of the 100G ports are not created. [PR1343970](#)
- When a **request system reboot now** is triggered it can take 10 seconds for the interfaces to go down. [PR1344831](#)
- When you deactivate or activate IRB with VRRP configuration in a scaled setup with 1000 VRRP groups, convergence time will be 10 to 30 seconds. [PR1345272](#)

Routing Protocols

- Configuring link aggregation group (LAG) hashing with the **[edit forwarding-options enhanced-hash-key] inet vlan-id** statement uses the VLAN ID in the hashing algorithm calculation. On some switching platforms, when this option is configured for a LAG that spans FPCs, such as in a Virtual Chassis or Virtual Chassis Fabric (VCF), packets are dropped due to an issue with using an incorrect VLAN ID in the hashing algorithm. As a result, the **vlan-id** hashing option is not supported in a Virtual Chassis or VCF containing any of the following switches as members: QFX5100, or QFX5110 switches. Under these conditions, use any of the other supported **enhanced-hash-key** hashing configuration options instead. [PR1293920](#)
- The route unidimensional limit is 1.6 million routes in Junos OS Release 18.1R1. [PR1320865](#)
- If you configure GRE tunneling with the underlying ECMP nexthop instead of a unicast nexthop, traffic might be dropped. This scenario is not supported. [PR1332309](#)

Services Applications

- You cannot configure analyzers on QFX10002-60C switches. The CLI configuration command **set forwarding-options analyzer** and the CLI operational command **show forwarding-options analyzer** are not supported on the switch.

Storage and Fibre Channel

- If the configuration changes or any aggregation devices (AD) restart, you might see inconsistency in the output of **show ethernet-switching table** and **show fip snooping satellite** on different ADs for some time. It takes time for the ADs to completely restart and hence MAC addresses might be learned over EVPN (DRP flag). When AD restart is complete, MAC addresses should be learned locally and hence the DRP flag moves to the S flag. It might take up to 10 minutes to get consistent output for **show** commands. The output for **show ethernet-switching table** on all ADs will show all the MAC addresses. However, the flags against the MAC addresses might be different on the ADs because the MAC addresses might be learned statically on some ADs and dynamically on others. The flag against the dynamic MAC addresses will be changed from D to S once those MAC addresses are relayed from the satellite device (SD) to the AD, which can take up to 10 minutes. However, there should not be any traffic drop. Traffic drop is expected only initially, when the AD has just been restarted. [PR1304173](#)

SEE ALSO

[New and Changed Features | 208](#)

[Changes in Behavior and Syntax | 227](#)

[Known Issues | 234](#)

[Resolved Issues | 240](#)

[Documentation Updates | 248](#)

[Migration, Upgrade, and Downgrade Instructions | 249](#)

[Product Compatibility | 263](#)

Known Issues

IN THIS SECTION

● [EVPN | 235](#)

● [Interfaces and Chassis | 235](#)

- [Layer 2 Features | 235](#)
- [MPLS | 235](#)
- [Platform and Infrastructure | 236](#)
- [Routing Protocols | 239](#)

This section lists the known issues in hardware and software for the QFX Series switches in Junos OS Release 18.1R2.

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

EVPN

- The error message **JPRDS_DLT_ALPHA KHT** shows as failed, but the entries in the hardware are programmed correctly. This might cause confusion regarding working and non-working conditions. [PR1258933](#)
- In an EVPN collapsed L2/L3 multihomed GWs topology, when traffic is sent from IP fabric towards EVPN, some traffic loss is seen. If the number of hosts behind EVPN gateways is increased, the traffic loss becomes higher. This issue is seen with QFX10000. [PR1311773](#)
- On a scaled EVPN-VXLAN setup, loading the scaled configuration and the base configuration alternately for a few times, might result in losing adjacency and hence the protocols will be down. [PR1349659](#)

Interfaces and Chassis

- Difference in error message reporting is observed when 100g and 40g is configured in a LAG, QFX10002-72Q error messages are more meaningful than QFX10002-60C error messages. [PR1340974](#)

Layer 2 Features

- QFX5210: Issues with the latency tests: 10G latency values of cut-through are higher than store and forward, in the 40G latency test for the frame size 1280 higher latency value is noticed. [PR1343579](#)

MPLS

- There might be some lingering RSVP state that would keep some labeled-routes programmed in the Packet Forwarding Engine longer than they should be. This RSVP state will eventually expire and then

delete the RSVP MPLS routes from FIB. However, no traffic loss is anticipated due to this lingering state or the corresponding label routes in the FIB. In the worst case, in a network where there is persistent link flapping going on, this lingering state might interfere with the LSP scale being achieved. [PR1331976](#)

- QFX5210: Scale: Error messages **BRCM_NH-,brcm_nh_mpls_action_uninstall(),3087:Reason ipv4 to mpls nh uninstall failed** are noticed when the RSVP Ingress scaled configurations are deleted. [PR1345480](#)
- The traffic loss was more than 50ms while performing FRR. The traffic loss was well within 50ms during FRR. However, the head-end node is re-signaling tunnels on the Primary path for failure detection and switching traffic to new tunnels, while the transit LSR (QFX5210-64C) has not fully completed tunnel installation. Hence, more packet drop is observed during the overall FRR event. [PR1345843](#)

Platform and Infrastructure

- L3 multicast traffic does not converge to 100 percentage and a few continuous drops are observed after bringing an interface down and back up again or while an FPC comes online after FPC restart. This behavior is seen when scaling beyond 2000 VLANs or 2000 IRBs with VLAN replication configured. [PR1161485](#)
- When per-packet load balancing is removed or deleted, the next-hop index might change. [PR1198092](#)
- On QFX10000 line switches, at initialization, the port group module comes up after some time and negative ACKs are seen until the port group module is up. Once the port group module is up, negative ACKs are no longer observed. [PR1271579](#)
- On QFX10000 line platforms, with a high scale of 4000 VNIs or 200,000 MACs or both, if a 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 might increase system load. [PR1296089](#)
- In an L2/L3 collapsed EVPN-VXLAN scenario, even though all the remote MACs learned, more than 60 percent of the traffic is flooded for L2 VNI stretched between PODs with the same subnet but different VLAN-to-VNI mapping [PR1303598](#)
- On QFX5110 switches, digital optical monitoring (DOM) status through the CLI is not correct in Junos OS Release 15.1X53 through 17.1x. The light level statistics might be seen in the FPC shell level. It has no traffic impact. [PR1305506](#)
- Traffic drop occurs on sending traffic over "et" interfaces due to CRC errors. [PR1313977](#)
- Family Ethernet-switching cannot be used when **flexible-vlan-tagging** is configured. The behavior is nondeterministic with this configuration and there is a possibility of seeing a dcpfe core file. [PR1316236](#)
- Port LEDs on QFX5100 do not work. If a device connects to a port on QFX5100, the port LED stays unlit. [PR1317750](#)
- IRB interface is not supported on VXLANs that have **igmp-snooping** configured. If IRB is configured, then a dcd restart could lead to multicast traffic loss. [PR1322057](#)

- On a QFX10016, permanent traffic loss is seen for some hosts after the initial ARP timer expiry caused by an ARP entry is not synchronized between the 2 PE devices. [PR1322288](#)
- In a MH EVPN-VXLAN scenario, with **igmp-snooping** configured, in a scaled scenario:
 For 10000 s,g scale —The triggering event is to disable DF link for convergence: Total convergence for 10,000 s,g scale is 4.5 seconds with traffic rate of 60kpps. Per-flow convergence loss ranges from 3.16 seconds to 5.66 seconds.
 For 8000 s,g scale: The triggering event is to disable DF link for convergence: Total convergence for 8000 s,g scale is 2.86 seconds with traffic rate of 60 kpps. Per-flow convergence loss ranges from 1.86 seconds to 3.73 seconds. [PR1323155](#)
- QFX5210: No Prune to RP was sent from LHR after shifting to GR Interface, when RP is in transit node [Multicast over GRE Tunnel Scenario]. [PR1323620](#)
- Traffic statistics for multicast stream on GR interfaces does not work on QFX5000 platform. [PR1323622](#)
- Interface uptime has increased by 8 seconds from Junos OS Release 17.4R1 release to 18.1R1 release. [PR324374](#)
- 100G DAC/copper cable connected between QFX5210-64C and QFX10000 devices, links might not come up reliably. The rest of the 100G Optics/AOC, 40G Optics/DAC/Copper work well when connected between QFX5210-64C and QFX10000 devices. [PR1324600](#)
- Persistent MAC is not enabled. [PR1325313](#)
- QFX10002-60C filter operation with log action is not supported for protocols other than L2/IPv4/IPv6, and the message **Protocol 0 not recognized** is seen in firewall logs. [PR1325437](#)
- The management process (mgd) might panic after modifying aggregated Ethernet interface members under **ethernet-switching vlan** stanza. After mgd panic, your remote session is terminated as a result. [PR1325736](#)
- Analyzer is not supported in QFX10002-60C. [PR1327288](#)
- Additional check was needed to ensure that the new .local, pseudo logical interface (IFL) gets correctly installed on the remote peer PE device only for ARP entries. [PR1330663](#)
- BFD session over aggregated Ethernet flaps when member link is carrying the BFD Tx flaps. [PR1333307](#)
- In a corner case, rpd generates core files during resolution of VPN label-route in MPLS.0 table. This label is allocated for the route in VRF learnt from remote PE. Also, VRF is configured with no-vrf-propagate-ttl. [PR1334846](#)
- Changing MTU for GRE and underlying interfaces in single commit has limitations for the RLI
 QFX10000-60C : QFX: PFE: IP GRE . Refrain from committing MTU changes for GRE and underlying interfaces in single commit. As a workaround, for any GRE interface MTU update, commit MTU changes for GRE and underlying interfaces together in separate commits with some time gap between the two commits. [PR1335739](#)

- qfx10k(1) - 172.15.0.2 - vip 172.15.0.1 (subinterface xe-0/0/3:3.700) qfx5100(1) - 172.15.0.4 - vip 172.15.0.6 (IRB.700) qfx5100(2) - 172.15.0.5 - vip 172.15.0.6 (IRB.700) qfx10k(2) - 172.15.0.3 - vip 172.15.0.1 (subinterface xe-0/0/3:3.700) #run show vrrp Interface State Group VR state VR Mode Timer Type Address xe-0/0/3:3.700 up 100 master Active A 0.710 lcl 172.15.0.2 vip 172.15.0.1 A full mesh ping works:), except for the - vip 172.15.0.1. Only Master can ping 172.15.0.1 (either qfx10k-1 or qfx10k-2 same issue seen). VRRP works as expected If is implemented with IRBs on all devices, it works as expected. Resolved in 17.3R1-S5,18.3,17.4R2.
- Changing MTU for GRE and underlying interfaces in single commit will be a caveat for the IPv4 GRE feature. Refrain from committing MTU changes for GRE and underlying interfaces in single commit. As a workaround, for any GRE interface MTU update, commit MTU changes for GRE and underlying interfaces together in separate commits with some time gap between the two commits. [PR1339601](#)
- In a 7-node topology and when BGP is not configured in a mesh network, there is a 5 percent multicast/broadcast traffic loss in the leaf (QFX5100) nodes. [PR1343809](#)
- On upgrading QFX10002 from Junos OS Release 15.1X53-D66 to Release 18.1R1, some of the 100G ports are not created. [PR1343970](#)
- In an MC-LAG with VRRP topology, when the master node is coming up after reboot, traffic going through other node also gets affected for few seconds. [PR1344286](#)
- With all timers enabled for high availability (HA) the drop should be minimal for MC-LAG node reboot when the node goes down or while the node is coming up for the traffic bound from hosts connected to the L2 switch below the MC-LAG node to the L3 core node. [PR1344589](#)
- Incorrect inner VLAN tag is sent from QFX10000 platform when double VLAN tags are configured on the Layer 3 sub interface (also called Layer 3 logical interface). It will cause traffic drop. [PR1346371](#)
- Error messages are seen after configuring multiples interfaces under the protocol sflow, and these errors are related to sFlow Bindpoint set error and related to lookup failed **IFD_EGRESS_IMPL_FILTER** on doing commit. Whenever you perform any commit on QFX10002, these errors message will get logged in syslog. [PR1346493](#)
- Starting in Junos OS Releases 14.1X53-D46, 15.1R7, 16.1R6, 17.1R3, 17.2R3, 17.2X75-D90, 17.3R2,18.1R1,18.1X75-D10, and later, the QFX5100-48T 10G interface might be auto-negotiated at 100M speed instead of 10G after peer device reboot. [PR1347144](#)
- If 25G channelisation is reapplied with an MC-LAG configuration repeatedly dcpfe generates a core file. This issue is rarely seen.[PR1348518](#)
- With the Junos OS Releases 18.1R1 image, when QFX5000 and QFX10000 line switches are upgraded through ZTP, configuration commit might fail if the configuration is fetched through a Python script. [PR1349240](#)

Routing Protocols

- On QFX5100 switches with Q-in-Q, if the native VLAN is configured on a Q-in-Q interface connected to a customer device (CE), the packets going out with the native VLAN ID (customer VLAN) are still tagged. [PR1105247](#)
- On QFX10000 line platforms, during route next-hop churn or earliest deadline first (EDF) job priority changes, memory corruption might occur, leading to processing issues and constant packet drop. [PR1243724](#)
- For the QFX10002 and QFX10008 switches, you might observe an increase in the convergence time of OSPF routes when compared to Junos OS 17.3 releases. An average increase of 1.5 seconds is seen for 100,000 OSPFv3 routes. [PR1297541](#)
- Performing GRES on the EVPN-VXLAN topology with uRPF results in total packet loss. [PR1322217](#)
- In the P-VLAN configuration, the isolated VLAN and community VLAN should not use same VLAN ID. [PR1323520](#)
- VLAN range shown in community VLAN is 1..4094. Hence, VLAN 0 should not be configured as community VLAN in P VLAN. [PR1323719](#)
- When MoFRR is enabled, traffic statistics on multicast route shows double the outgoing traffic. Accounting is done for both the primary and the backup route; hence the issue. When one of the upstream interfaces goes down, this issue will not be seen. [PR1326338](#)
- When cleaning up routes as the peer goes down, a 30 percent degradation is observed in time taken in 17.2X75-D91 as compared to the 17.2 release. [PR1329921](#)
- Higher convergence time for LFA with BFD in Junos OS Release 18.1 is noticed. [PR1337412](#)
- On QFX5210, when ICCP/ICL link is disabled or enabled, data-driven ARP learning is taking 2-3 seconds longer than on QFX5200-32C, leading to ~10 seconds of IPv4/IPv6 traffic loss . [PR1338444](#)
- If a permanent traffic loop is created in IP-CLOS topology, Packet Forwarding Engine CPU utilization might go high, which can result in ping drops. [PR1341107](#)
- DF is not working as expected. [PR1345495](#)

SEE ALSO

[New and Changed Features | 208](#)

[Changes in Behavior and Syntax | 227](#)

[Known Behavior | 229](#)

[Resolved Issues | 240](#)

[Documentation Updates | 248](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 18.1R2 | 240](#)
- [Resolved Issues: 18.1R1 | 243](#)

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: 18.1R2

EVPN

- Sub interface from the same physical port do not work if configured under same VXLAN VLAN. [PR1278761](#)
- VXLAN traffic loss is observed after deleting and adding VLANs. [PR1318045](#)
- QFX5100: EVPN-VXLAN: leaf device forwarding traffic to the incorrect VTEP after MAC move / vmotion. [PR1335431](#)
- Configuration of VXLANs with and without **encapsulate-inner-vlan** cannot co exist causing traffic issues on access interfaces. [PR1337953](#)
- In EVPN/VXLAN environment, BFD flaps cause VTEP flaps and cause the Packet Forwarding Engine to crash [PR1339084](#)
- The rpd generates a core file on QFX Series switches with multiple VLANs with vlan-id zero, unique VNID. [PR1342351](#)

Interfaces and Chassis

- CVLANs range is 16 might not pass traffic in a Q-in-Q scenario. [PR1345994](#)

Layer 2 Features

- QFX5100: With multiple logical units configured on an interface, **input-vlan-map POP** is not removing outer vlan-tag when QinQ and VXLAN are involved. [PR1331722](#)
- Push is not working for VXLAN local switching with the QinQ. [PR1332346](#)
- Interface with **flexible-vlan-tagging** and **family ethernet-switching** does not work on the QFX10000 line.. [PR1337311](#)

MPLS

- The hot standby for I2circuit does not work on QFX5100, QFX5110, and QFX5200. [PR1329720](#)

Platform and Infrastructure

- C0 fiber link does not come up. [PR1298876](#)
- Packets such as TDLS without IP headers are looped between virtual gateways. [PR1318382](#)
- Autonegotiation is not working as expected between EX4300 and SRX5800. [PR1318382](#)
- The openflow session cannot be established correctly with controller and interfaces options configured on QFX5100 series switches. [PR1323273](#)
- The GRE traffic is not decapsulated by the firewall filter. [PR1325104](#)
- VLAN or VLAN bridge might not be added or deleted if there is an IFBD hardware token limit exhaustion. [PR1325217](#)
- Deleting one VXLAN might cause traffic loop on another VXLAN in a multihoming EVPN-VXLAN scenario with service provider style interface. [PR1327978](#)
- 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 PTX10000 line card might reboot continuously after upgrading to Junos OS Release 17.2R1 or later if HMC BIST fails. [PR1330618](#)
- DHCP relay/server is not working on GRE interface on QFX10002-36Q (Elit). [PR1331158](#)
- PTP BC with its PTP slave interface configured on a 100-Gigabit Ethernet interface might get stuck in FREERUN state. [PR1331752](#)
- EVPN-VXLAN: DF drops multicast traffic. [PR1333069](#)
- Chassis reboots continuously when USB drive is connected after image recovery through USB and after CLI image install. [PR1335269](#)
- PTX1000 and QFX10002-60C: Python scripts/shell scripts cannot be executed during ZTP because verixec is enabled. [PR1334425](#)

- Supported scale for logical interface (IFL) based GRE tunnel on QFX10002-60C is 512. [PR1335681](#)
- SNMP jnxBoxDescr oid returns different value when upgrading to Junos OS Release 17.2. [PR1337798](#)
- The traffic coming from the remote VTEP PE device might be dropped. [PR1338532](#)
- The analyzer status might show as down when port mirroring is configured to mirror packets from an AE member. [PR1338564](#)
- The VXLAN traffic might not be transmitted correctly with IRB interface as underlay interface of VTEP tunnel. [PR1338586](#)
- DDOS counters for OSPF might not increment. [PR1339364](#)
- Reduced multicast scale with downstream IRB interfaces with snooping enabled. [PR1340003](#)
- QFX5200: Inconsistent result occurs after using **deactivate xxx** command in pfc-priority and no-loss context. [PR1340012](#)
- JDI-RCT : QFX5210-64C : IPv4 traffic routed out through the incorrect interface after rpd restart in leaf of IPCLOS profile. [PR1341381](#)
- While downgrading PTX from a later release, the router goes into amnesiac state. [PR1341650](#)
- JDI-RCT: EVPN-VXLAN: L3 traffic is not getting converged properly upon disabling the ECMP link between the spine and leaf devices with EVPN-VXLAN configurations. [PR1343172](#)
- Broadcast frames might be modified with the ethertype 0x8850. [PR1343575](#)
- EVPN-VXLAN: VLAN with flexible-tag mode , the xe statistics do not get updated for ingress traffic. [PR1343746](#)
- Implement **edit interfaces interface-name ether-options] configured-flow-control** option for QFX Series switches. [PR1343917](#)
- EVPN-VXLAN: ARP reply packet has auto generated virtual gateway MAC in Ethernet header. [PR1344990](#)
- The fxpc process might generate core files when removing a VXLAN configuration. [PR1345231](#)
- EVPN Type5: QFX5110 dcpfe generates core files at `src/pfe/common/pfe-arch/brcm/applications/virtual/brcm_vxlan.c:2185`. [PR1346980](#)
- Part numbers and serial numbers are not displayed for any of the optics/DAC connected. [PR1347634](#)
- The ARP might not update and packets might get dropped at the Routing Engine. [PR1348029](#)
- On the QFX10002-60C VMHOST, a crash was observed at `@ prds_if_ifl_get_gre_stats (ifl=0x9288a608, expr_ifl_l2d_stats=0x2cd3790c)`, just after configuring the GR Interface on it. [PR1348932](#)
- The pfed process is consuming 80-90 percent CPU usage when running subscriber management on PPC-based routers. [PR1351203](#)
- The GTP traffic might not be hashed correctly for aggregated Ethernet interface. [PR1351518](#)

Routing Protocols

- Diffserv bits/ToS bits are not getting copied from the inner IP header to GRE header, Wireshark captured attached with PR. [PR1313311](#)
- Some of the IPv4 multicast routes in the Packet Forwarding Engine might fail to install and update. [PR1320723](#)
- The dcpfe crash is seen in route leak scenario on QFX10000. [PR1334714](#)
- The rpf-check-policy does not work as expected. [PR1336909](#)
- QFX loopback firewall filter is not able to catch packets with martian source address. [PR1343511](#)
- vrf-fallback on the QFX5100 switch, is not supported in ALPM mode. [PR1345501](#)
- IPv6 packets with hop-by-hop header are not matched by filters. [PR1346052](#)

Resolved Issues: 18.1R1

Class of Service (CoS)

- For some of the frame sizes, throughput is not 100 percent. [PR1256671](#)

EVPN

- NH installation error messages are seen on QFX10000 .[PR1258930](#)
- VXLAN-EVPN: IPv6 Packet loss after normal traffic run rate. [PR1267830](#)
- Normal VRRP MAC is triggering a MAC move, and logical interfaces on the BD are getting shut down. [PR1285749](#)
- QFX10002 VXLAN with MPLS underlay has traffic loss at RSVP egress.[PR1289666](#)
- The **df-election-type** preference statements at the [**show interfaces esi**] hierarchy level are not supported on QFX10000 running Junos OS Release 17.3R1. [PR1300093](#)
- QFX5110-48S: L3 VPN traffic is dropped for some instances when EVPN-VXLAN configuration is removed and reapplied. [PR1307590](#)
- Dcpfe might crash on EVPN-VXLAN setup. [PR1315531](#)
- Core file link flap might result in inconsistent global MAC count. [PR1328956](#)
- EVPN-VXLAN: EVPN Type7 route is not synced across ESI peers when virtual-switching or EVPN instance exist. [PR1334408](#)
- QFX5100 -- EVPN-VXLAN -- Leaf forwarding traffic to incorrect VTEP after MAC move / vmotion. [PR1335431](#)

Interfaces and Chassis

- Multicast data packets are looping in MC-LAG. [PR1281646](#)
- ARP reply drop occurs in MC-LAG scenario. [PR1282349](#)

- Upgrading to Junos OS Release 16.1R5 without the **redundancy-group-id-list** statement prior in ICCP leads to commit failure during bootup. [PR1311009](#)

Layer 2 Features

- To set up PTP BC forwarding on a QFX10002, configure routing on the interface or add a static ARP entry on the remote PTP device. [PR1275327](#)
- Device transmits packets that exceed interface MTU. [PR1306724](#)
- The **bpdu-block-on-edge** statement does not work correctly when **fast-tune** is enabled. [PR1307440](#)
- jdhcpd core files are observed after making DHCP configuration changes. [PR1324800](#)
- Commit error occurs while configuring **native-vlan-id**. [PR1318881](#)
- NLB heartbeat packets might be dropped on QFX10000 and PTX Series. [PR1322183](#)
- ARP entry might be learned on STP blocking ports. [PR1324245](#)
- Junos Fusion MAC Learning failure occurs for device on Extended Satellite Interface. [PR1324579](#)
- The DHCP discover packets might be looped in an MC-LAG and DHCP-relay scenario. [PR1325425](#)
- QFX5100 : With multiple logical units configured on an interface, " input-vlan-map POP " is not removing outer vlan-tag when QinQ and VXLAN are involved. [PR1331722](#)
- Interface with **flexible-vlan-tagging** and **family ethernet-switching** does not work on QFX10K. [PR1337311](#)

MPLS

- QFX5100: ISSU is not supported with MPLS configuration. [PR1264786](#)
- Traffic drop during NSR switchover for RSVP P2MP provider tunnels used by MVPN occurs. [PR1293014](#)
- DHCP clients cannot get IP address over BGP-L3VPN. [PR1303442](#)
- MPLS forwarding might not happen properly for some LSPs. [PR1319379](#)
- The rpd might crash on backup RE due to memory exhaustion. [PR1328974](#)
- Hot standby for I2circuit does not work on QFX5100. [PR1329720](#)

Multicast

- aggregated Ethernet interface and IRB configuration issue causes kernel crash and causes either chassis or FPC to reboot. [PR1335904](#)

Platform and Infrastructure

- UFT for non local member is not shown in the CLI. [PR1243758](#)
- 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](#)
- Copper ports flap on QFX5100-48T when short-reach-mode is enabled. [PR1248611](#)

- After upgrading the QFX5100/EX4600 to Junos OS Release 16.1 from 15.1, commit warning. `/boot/ffp.cookie+` might be seen. [PR1283917](#)
- On QFX5100 switches, an AE interface might flap upon commit if an explicit speed is configured on an AE member interface. [PR1284495](#)
- BFD sessions might flap when BFD is configured over IRB interfaces. [PR1284743](#)
- Protocols might flap when disabling the AE member link. [PR1289703](#)
- Storm-control flags are not set after a Routing Engine switchover. [PR1290246](#)
- On QFX5100, the fxpc process generates a core file. [PR1294033](#)
- ULC-60S-6Q LC on QFX10008: The port becomes unusable after inserting a third-party SFP-T optic. [PR1294394](#)
- Oinker and TCP connection drop might be seen during large file SCP/FTP to the system (high `intr{virtio_p}` seen). [PR1295774](#)
- The 40-Gigabit Ethernet interface might not come up if a specific vendor's DAC cable is used. [PR1296011](#)
- The disable-pfe action upon hybrid memory cube (HMC) fatal errors might have a system-wide impact on PTX Series platforms. [PR1300180](#)
- QFX10008/10016: commit error is seen when configured with mixed speed. [PR1301923](#)
- 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](#)
- Systems running 32-bit Junos OS might generate rpd core file when traceoptions are enabled. [PR1305440](#)
- QFX5110-48S: Digital optical monitoring statistics cannot be received through the CLI in Junos OS Releases 15.1X53 through 17.x. [PR1305506](#)
- QFX5200: New apply group is not applying to the Virtual Chassis after a reboot. [PR1305520](#)
- QFX5100 crashes and the fxcp process generates a core file. [PR1306768](#)
- Some error messages might be observed on EVPN-VXLAN setup. [PR1307014](#)
- QSFP+4x10G-IR channelized interface goes down between QFX5200 and PTX5000. [PR1307400](#)
- Traffic stopped passing LSP after MPLS route change. [PR1309058](#)
- QFX5110 VC/VCF: Virtual Chassis members reboot before all members have image installed. [PR1309103](#)
- Run time pps statistics value might show zero for a subinterface of AE interface. [PR1309485](#)
- Traffic loss might be seen if sending traffic through the 40G interface. [PR1309613](#)
- Some log messages are seen on QFX5110 platform when plugging in an SFP-SX. [PR1311279](#)
- One aggregated Ethernet member does not send out sFlow sample packets. [PR1311559](#)
- The FPC memory might be exhausted with SHEAF leak messages seen in the syslog. [PR1311949](#)
- Traffic loss is observed while performing NSSU. [PR1311977](#)

- CPU utilization is around 50 percent without any configuration. [PR1312520](#)
- QFX5100:5100-24q: After loading TVP image, unable to offline/online the EX4600-EM-8F PIC; shows as unsupported. [PR1313392](#)
- QFX10002-60C will support **show vmhost crash** to display core files in the host OS. [PR1314451](#)
- Transit traffic over GRE tunnel might hit CPU and trigger a DDoS violation on L3NHOP. [PR1315773](#)
- On switch platforms running under Junos OS with Enhanced Layer 2 Software (ELS) (EX4300/EX4600/EX9200/QFX5100/QFX10000), I2cpd might generate core files repeatedly if an interface is connected to VoIP product with LLDP and LLDP-MED enabled. [PR1317114](#)
- 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](#)
- Port speed is still showing 100G instead of 50G as IFD has been channelized to 50G. [PR1319884](#)
- Chassis MIB SNMP OIDs for VC-B member chassis are not available after MX-VC ISSU. [PR1320370](#)
- The MACac address is stuck with "DR" flag on the spine node even though packets are received on the interface from source MAC. [PR1320724](#)
- FPCs are gone offline due to **CHASSISD_IPC_CONNECTION_DROPPED: Dropped IPC connection for FPC**. [PR1321198](#)
- The openflow session cannot be established correctly with controller on QFX5100 Series switches. [PR1323273](#)
- Update new firmware versions for jfirmware package for 100G-PSM4 and 100G-AOC issues. [PR1323321](#)
- EVPN Type 5: Unicast traffic getting is dropped on backup forwarder [PR1323907](#)
- VLAN or VLAN bridge might not be added or deleted if there is an IFBD HW token limit exhaustion. [PR1325217](#)
- MAC move is not expected when disabled globally with **set protocols l2-learning global-mac-move disable-action** [PR1325524](#)
- ARP request packets might not be flooded on QFX5110. [PR1326022](#)
- QFX5210-64C When the physical interface is down, **show chassis LED** CLI still showing as "Green". [PR1326078](#)
- QFX5100/EX4600/ACX5k: Major Alarm **Fan & PSU Airflow direction mismatch** occurs when removing 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](#)
- Major alarm should be cleared once the chassis has more PEM units installed than the "minimum PEM" configuration. [PR1327999](#)

- Junos automation folder lost execution permissions. [PR1328570](#)
- Fan tray removal/insertion trap is not generated for the backup FPC. [PR1329031](#)
- QFX10000-60C : Although the set chassis fpc 0 pic command has the option of PIC numbers 0 to 2 , the switch has only 1 PIC.[PR1329105](#)
- After commit, members of VC or VCF are split and some members may get disconnected. [PR1330132](#)
- When configure total of 500 tunnels and all are part of routing-instance (500 routing-instance) and 500 BGP session with 20k routes. Adding or deleting configurations might occasionally result in FPC crash. [PR1331983](#)
- The error messages **out of HMC range** and **HMC READ failed** are seen. [PR1332251](#)
- The SOLICIT message of DHCPv6 is dropped. [PR1334680](#)
- Supported scale for IFL based GRE tunnel on QFX10002-60C is 512. [PR1335681](#)
- PTX1000 & QFX10002-60C: Python scripts/shell scripts cannot be executed during ZTP as verixec is enabled.[PR1334425](#)
- CLI for beacon port state is not supported on QFX10002-60C. [PR1337125](#)
- The traffic coming from the remote VTEP PE might be dropped. [PR1338532](#)
- QFX5200 : Inconsistent result after using 'deactivate xxx' command on 'pfc-priority' and 'no-loss' context. [PR1340012](#)
- Implement **edit interfaces interface-name ether-options] configured-flow-control** option for QFX. [PR1343917](#)
- When upgrading from certain release to 18.1R1 statistics daemon PFED may be seen to core. This issue is not service impacting. The issue can be cleared by rebooting the chassis or by deleting all files from /mfs. [PR1346925](#)

Routing Policy and Firewall Filters

- The rpd might crash if **vrf-target auto** is configured under routing-instance [PR1301721](#)

Routing Protocols

- Filter-based forwarding (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 is offlined.[PR1290500](#)
- 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](#)
- GRE tunneled packets might be dropped. [PR1308438](#)
- QFX5100: Consistent hashing is not getting programmed. [PR1322299](#)

- QFX10002-60C is not supported as FHR in multicast PIM SM based network. [PR1324116](#)
- IS-IS L2 Hello packets are dropped when they come from a Brocade device. [PR1325436](#)
- vrf-fallback on QFX5K is not supported in ALPM mode. [PR1345501](#)

Virtual Chassis

- Sometimes multicast packets are received two or three time faster. [PR1306239](#)

SEE ALSO

[New and Changed Features | 208](#)

[Changes in Behavior and Syntax | 227](#)

[Known Behavior | 229](#)

[Known Issues | 234](#)

[Documentation Updates | 248](#)

[Migration, Upgrade, and Downgrade Instructions | 249](#)

[Product Compatibility | 263](#)

Documentation Updates

IN THIS SECTION

- [New Simplified Documentation Architecture | 248](#)

There are no documentation errata or changes for the QFX Series switches in Junos OS Release 18.1R2.

New Simplified Documentation Architecture

- With the release of Junos OS Release 18.1, Juniper is simplifying its technical documentation to make it easier for you to find information and know that you can rely on it when you find it. In the past, we organized documentation about Junos OS software features into platform-specific documents. In many cases, features are supported on multiple platforms, so you might not easily find the document you want for your platform.

With Junos OS Release 18.1, we have eliminated the platform-specific software feature documents. For example, if you want to find documentation on OSPF, there is only one document regardless of which platform you have. Here are some of the benefits of our new simplified architecture:

- Over time, you will see better search results when looking for Juniper documentation. You will be able to find what you want faster and be assured that is the right document.
- If a software feature is supported on multiple platforms, you can find information about all the platforms in one place.
- Because we have eliminated many documents that covered similar topics, you will now find one document with all the information.
- You can know that you are always getting the most current and accurate information.

SEE ALSO

[New and Changed Features | 208](#)

[Changes in Behavior and Syntax | 227](#)

[Known Behavior | 229](#)

[Known Issues | 234](#)

[Resolved Issues | 240](#)

[Migration, Upgrade, and Downgrade Instructions | 249](#)

[Product Compatibility | 263](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrading Software on QFX Series Switches | 250](#)
- [Installing the Software on QFX10002-60C Switches | 252](#)
- [Installing the Software on QFX10002 Switches | 252](#)
- [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 | 253](#)
- [Installing the Software on QFX10008 and QFX10016 Switches | 255](#)
- [Performing a Unified ISSU | 259](#)
- [Preparing the Switch for Software Installation | 260](#)

- Upgrading the Software Using Unified ISSU | 260
- Upgrade and Downgrade Support Policy for Junos OS Releases | 262

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://www.juniper.net/support/downloads/junos.html>.

The Junos Platforms Download Software page appears.

2. In the QFX Series section of the Junos Platforms Download Software page, select the QFX Series platform for which you want to download the software.
3. Select **18.1** 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 18.1 release.

An Alert box appears.

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

A login screen appears.

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

8. Copy the software to the device or to your internal software distribution site.
9. Install the new jinstall package on the device.

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

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

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-18.1  
-R1.n-secure-signed.tgz reboot
```

Replace **source** with one of the following values:

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 18.1 **jinstall** package, you can issue the **request system software rollback** command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

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

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

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

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

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

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

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-18.1R2.9.tgz
```

If the Install Package resides remotely from the switch, execute the **request vmhost software add <pathname><source>** command.

For example:

```
user@switch> request vmhost software add
ftp://ftpserver/directory/junos-vmhost-install-qfx-x86-64-18.1R2.9.tgz
```

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

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

Installing the Software on QFX10002 Switches

NOTE: If you are upgrading from a version of software that does not have the FreeBSD 10 kernel (15.1X53-D30, for example), you will need to upgrade from Junos OS Release 15.1X53-D30 to Junos OS Release 15.1X53-D32. After you have installed Junos OS Release 15.1X53-D32, you can upgrade to Junos OS Release 15.1X53-D60 or Junos OS Release 18.1R1.

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-x86-64-18.1R2.n-secure-signed.tgz reboot
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> reboot** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-f-x86-64-18.1R2.n-secure-signed.tgz reboot
```

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

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

Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at <https://www.juniper.net/support>.

The switch contains two Routing Engines, so you will need to install the software on each Routing Engine (re0 and re1).

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

To install the software on re0:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> re0** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

To install the software on re1:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> re1** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

Reboot both Routing Engines.

For example:

```
user@switch> request system reboot both-routing-engines
```

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

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

Installing the Software on QFX10008 and QFX10016 Switches

Because the switch has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at <https://www.juniper.net/support>.



WARNING: If graceful Routing Engine switchover (GRES), nonstop bridging (NSB), or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you issue the CLI **delete chassis redundancy** command when prompted. If GRES is enabled, it will be removed with the **redundancy** command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the **[edit routing-options]** hierarchy level to disable it.

1. Log in to the master Routing Engine's console.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

2. From the command line, enter configuration mode:

```
user@switch> configure
```

3. Disable Routing Engine redundancy:

```
user@switch# delete chassis redundancy
```

4. Disable nonstop-bridging:

```
user@switch# delete protocols layer2-control nonstop-bridging
```

5. Save the configuration change on both Routing Engines:

```
user@switch# commit synchronize
```

6. Exit the CLI configuration mode:

```
user@switch# exit
```


After the switch has been prepared, you first install the new Junos OS release on the backup Routing Engine, while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the software version on the other Routing Engine.

7. Log in to the console port on the other Routing Engine (currently the backup).

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

8. Install the new software package using the **request system software add** command:

```
user@switch> request system software add validate
/var/tmp/jinstall-host-qfx-10-f-x86-64-18.1R2.n-secure-signed.tgz
```

For more information about the **request system software add** command, see the [CLI Explorer](#).

9. Reboot the switch to start the new software using the **request system reboot** command:

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

NOTE: You must reboot the switch to load the new installation of Junos OS on the switch.

To abort the installation, do not reboot your switch. Instead, finish the installation and then issue the **request system software delete <package-name>** command. This is your last chance to stop the installation.

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

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

10. Log in and issue the **show version** command to verify the version of the software installed.

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

Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the master Routing Engine software.

11. Log in to the master Routing Engine console port.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

12. Transfer routing control to the backup Routing Engine:

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

For more information about the **request chassis routing-engine master** command, see the [CLI Explorer](#).

13. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

```
user@switch> show chassis routing-engine
```

```
Routing Engine status:
Slot 0:
  Current state           Backup
  Election priority       Master (default)
Routing Engine status:
Slot 1:
  Current state           Master
  Election priority       Backup (default)
```

14. Install the new software package using the **request system software add** command:

```
user@switch> request system software add validate
/var/tmp/jinstall-host-qfx-10-f-x86-64-18.1R2.n-secure-signed.tgz
```

For more information about the **request system software add** command, see the [CLI Explorer](#).

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

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

NOTE: You must reboot to load the new installation of Junos OS on the switch.

To abort the installation, do not reboot your system. Instead, finish the installation and then issue the **request system software delete jinstall <package-name>** command. This is your last chance to stop the installation.

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

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

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

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

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

For more information about the **request chassis routing-engine master** command, see the [CLI Explorer](#).

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

```
user@switch> show chassis routing-engine
```

```
Routing Engine status:
  Slot 0:
    Current state           Master
    Election priority       Master (default)
Routing Engine status:
  Slot 1:
    Current state           Backup
    Election priority       Backup (default)
```

Performing a Unified ISSU

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

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

Perform the following tasks:

- [Preparing the Switch for Software Installation on page 260](#)
- [Upgrading the Software Using Unified ISSU on page 260](#)

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-x86-64-18.1R2.n-secure-signed.tgz*.

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

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

```
warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get
lost!
ISSU: Validating Image
ISSU: Preparing Backup RE
Prepare for ISSU
ISSU: Backup RE Prepare Done
Extracting jinstall-host-qfx-5-f-x86-64-18.1R2.n-secure-signed.tgz ...
Install jinstall-host-qfx-5-f-x86-64-18.1R2.n-secure-signed.tgz completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
```

```

ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status           Reason
  FPC 0          Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff

```

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

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

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

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

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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 17.1, 17.2 and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

SEE ALSO

[New and Changed Features | 208](#)

[Changes in Behavior and Syntax | 227](#)

[Known Behavior | 229](#)

[Known Issues | 234](#)

[Resolved Issues | 240](#)

[Documentation Updates | 248](#)

[Product Compatibility | 263](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 263](#)

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 208
Changes in Behavior and Syntax 227
Known Behavior 229
Known Issues 234
Resolved Issues 240
Documentation Updates 248
Migration, Upgrade, and Downgrade Instructions 249

Junos OS Release Notes for SRX Series

IN THIS SECTION

- [New and Changed Features | 265](#)
- [Changes in Behavior and Syntax | 271](#)
- [Known Behavior | 272](#)
- [Known Issues | 274](#)
- [Resolved Issues | 276](#)
- [Documentation Updates | 285](#)
- [Migration, Upgrade, and Downgrade Instructions | 286](#)
- [Product Compatibility | 287](#)

These release notes accompany Junos OS Release 18.1R2 for the SRX 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/software/junos/>.

New and Changed Features

IN THIS SECTION

- [Release 18.1R2 New and Changed Features | 265](#)
- [Release 18.1R1 New and Changed Features | 265](#)

This section describes the new features and enhancements to existing features in Junos OS Release 18.1R2 for the SRX Series devices.

Release 18.1R2 New and Changed Features

There are no new features in Junos OS Release 18.1R2 for the SRX Series devices.

Junos OS Release 18.1R2 supports the following Juniper Networks security platforms: vSRX, SRX300/320, SRX340/345, SRX550HM, SRX1500, SRX4100/4200, SRX4600, 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-D120. Security features delivered in Junos OS for SRX Series “X” releases after 15.1X49-D120 are not available in 18.1 releases.

Release 18.1R1 New and Changed Features

IN THIS SECTION

- [Application Security | 266](#)
- [Authentication and Access | 267](#)
- [Chassis Cluster | 267](#)
- [Class of Service \(CoS\) | 267](#)
- [Flow-Based and Packet-Based Processing | 267](#)
- [Interfaces and Chassis | 267](#)

- Multicast | 269
- Network Management and Monitoring | 269
- User Interface and Configuration | 269
- VPN | 269

Junos OS Release 18.1R1 supports the following Juniper Networks security platforms: vSRX, SRX300/320, SRX340/345, SRX550HM, SRX1500, SRX4100/4200, SRX4600, 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-D120. Security features delivered in Junos OS for SRX Series “X” releases after 15.1X49-D120 are not available in 18.1 releases.

Application Security

- **Data Loss Prevention (SRX Series)** —Starting in Junos OS Release 18.1, SRX Series devices support Data Loss Prevention (DLP) to redirect HTTP or HTTPS traffic to any server through Internet Content Adaptation Protocol (ICAP).

ICAP is a lightweight protocol for executing a remote procedure call on HTTP messages using **REQMOD** which encapsulate HTTP request messages and **RESPMOD** which encapsulate HTTP response messages.

See [SSL Proxy](#).

- **Optimizing SSL/TLS performance for HTTPS traffic (SRX Series, vSRX)** —Starting from Junos OS Release 18.1R1, SSL/TLS performance is optimized by minimizing the time required for performing the decryption by using the following methods:
 - Using optimized cipher suites
 - Maintaining the certificate cache

Enhanced SSL/TLS performance for HTTPS traffic results in improved website performance without compromising security, and maximizes user experience.

[See [SSL Proxy](#)].

- **SSL proxy support (SRX300, SRX320)**—Starting in Junos OS Release 18.1R1, SSL proxy support is available on SRX300 and SRX320 devices. SSL proxy acts as an intermediary, performing SSL encryption and decryption between the client and the server. SSL relies on digital certificates and private-public key exchange pairs for client and server authentication to ensure secure communication.

[See [SSL Proxy](#)].

Authentication and Access

- **IPv6 support for network access control (NAC) (SRX Series, vSRX)**—Starting with Junos OS Release 18.1R1, SRX Series devices support IPv6 for the network access control (NAC) system. You can configure a Web API client address with an IPv6 address and Web API supports IPv6 user or device entries obtained from Juniper Identity Management Service (JIMS). An SRX Series device can query JIMS periodically for batches of newly generated IPv6 users or devices for identity information. The SRX Series can query JIMS for identity information for an individual user or device based on the IPv6 address when the IPv6 traffic hits the SRX Series device. The SRX Series device firewall authentication can push IPv6 IP-user mapping information to JIMS.

[See [Understanding the SRX Series Advanced Query Feature for Obtaining User Identity Information from JIMS](#) .]

Chassis Cluster

- **VRRP and VRRPv3 support on redundant Ethernet interface to provide redundancy (SRX Series, vSRX)**—Starting with Junos OS Release 18.1R1, SRX Series devices in a chassis cluster support the Virtual Router Redundancy Protocol (VRRP) and VRRPv3 on reth interfaces to provide redundancy, route advertising, and load sharing. Using VRRP, a secondary node can take over a failed primary node within a few seconds with minimum VRRP traffic and without any interaction with the hosts.

[See [Understanding VRRP on SRX Series Devices](#).]

Class of Service (CoS)

- **Support for rewrite rules for both inner and outer VLAN tags on IEEE802.1 packets (SRX Series)**—Starting with Junos OS Release 18.1R1, SRX Series devices support applying rewrite rules to both inner and outer VLAN tags on IEEE802.1 packets. To apply rewrite rules to both inner and outer VLAN tags, set the **vlan-tag outer-and-inner** option at the **[edit class-of-service interfaces interface-name unit unit-number rewrite-rules ieee-802.1 rewrite-name]** hierarchy level.

[See [rewrite-rules \(CoS Interfaces\)](#)]

Flow-Based and Packet-Based Processing

- **Enhancement for show security flow statistics operational command (SRX Series, vSRX instances)**—Starting in Junos OS Release 18.1R1, the output of the **show security flow statistics** command has been modified. The **Packets forwarded** field has been split into the **Packets received** and **Packets transmitted** fields. The **Packets received** field displays the actual number of packets received, including those dropped by the system. The **Packet transmitted** field displays the number of packets returned to jexec for transmission. The **Packets forwarded/queued** field displays the actual number of packets forwarded excluding the dropped packets.

Additionally, a new field, **Packets copied** has been created to provide information about packets copied by other modules including fragmentation and TCP proxy.

[See [show security flow statistics](#).]

Interfaces and Chassis

- **Support for 4x10-Gigabit Ethernet Optical Breakouts (SRX4600)**—Starting in Junos OS Release 18.1R1, you can use optical breakout cable to configure four 10-Gigabit Ethernet interfaces on each 40-Gigabit Ethernet port on an SRX4600. By default, FPC 1 PIC 0 comes up with the default setting of four 40-Gigabit Ethernet ports. This new feature allows the 40 Gigabit Ethernet port to be configured in 4X10-Gigabit Ethernet mode by plugging in QSFP-4X10-Gigabit Ethernet optics connecting with 4x10-Gigabit Ethernet breakout cables. You use QSFP+ transceivers to connect the 40-Gbps (default speed) port to the breakout cable, which connects to four SFP+ transceivers at the other end thus converting that port into four 10-Gbps interfaces).

For example, on FPC 1 PIC 0, to configure each 40-Gbps port as four 10-Gbps interfaces, execute the **set chassis fpc 1 pic 0 pic-mode 10G** command.

After you commit the configuration, for the new configuration to take effect, you must reboot the device or chassis cluster. [See [SRX4600 Gateway Rate-Selectability Overview](#).]

- **Support for default 10-Gbps ports to operate at 1-Gbps speed (SRX4600)**—Starting in Junos OS Release 18.1R1, SRX4600 supports 1-Gbps port speed on the default 10-Gbps ports on its 8-port PICs and on two dedicated chassis cluster control ports on the 4-port chassis cluster PICs. The SRX4600 supports three different PIC types—8-port 10-Gigabit Ethernet PIC, 4-port 40-Gigabit or 100-Gigabit Ethernet PIC, and 4-port 10-Gigabit Ethernet PIC (in a chassis cluster). Out of the four ports on the 10-Gigabit Ethernet PIC in a chassis cluster, two ports are fabric ports and the other two ports are chassis cluster control ports. The two fabric ports do not support 1-Gbps speed. Only the two control ports of the chassis cluster support a port speed of 1 Gbps.

NOTE:

- The interface name prefix must be xe.
- You can configure a combination of 1-Gbps and 10-Gbps speed only on the 8-port 10-Gigabit Ethernet PIC. The chassis cluster control interfaces (that is, on the 4-port 10-Gigabit Ethernet PIC) do not support multiple speeds.

[See [SRX4600 Gateway Rate-Selectability Overview](#).]

Multicast

- **Layer 2 IGMP and MLD Snooping feature support (SRX1500)**—Starting with Junos OS Release 18.1R1, the SRX1500 supports the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) snooping feature in Layer 2 switching mode.

The snooping feature snoops the IGMP or MLD packets received by the switch interfaces and builds a multicast database. The SRX Series device uses the multicast database and forwards the multicast traffic only to the downstream interfaces of interested receivers. Using the multicast database to forward multicast packets helps ensure efficient use of network bandwidth.

[See [IGMP Snooping Overview](#) and [Understanding MLD Snooping](#).]

Network Management and Monitoring

- **Two-Way Active Measurement Protocol (TWAMP) support (SRX4100, SRX4200 and vSRX)**—Starting in Junos OS Release 18.1R1, the Two-Way Active Measurement Protocol (TWAMP) is supported on SRX4100 and SRX4200 devices and on vSRX instances in addition to the existing support on SRX Series devices such as SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500. TWAMP is a standard protocol framework that defines control and test session separation based on the client/server architecture. The TWAMP-Control protocol is used to set up performance measurement sessions between a TWAMP client and a TWAMP server, and the TWAMP-Test protocol is used to send and receive performance measurement probes.

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

User Interface and Configuration

- **Ephemeral configuration database support for load replace and load override operations (SRX Series)**—Starting in Junos OS Release 18.1R1, NETCONF and Junos XML protocol client applications can configure the ephemeral configuration database using **load replace** and **load override** operations, in addition to the previously supported **load merge** and **load set** operations. To perform a **load replace** or **load override** operation, set the **<load-configuration> action** attribute to **replace** or **override**, respectively.

[See [Configuring Ephemeral Database Instances](#).]

VPN

- **Binding trusted CAs or trusted CA group to an IKE policy (SRX Series and vSRX instances)**—Starting in Junos OS Release 18.1R1, you can group CA profiles (trusted CAs) in a trusted CA group and or bind a specific CA profile to an IKE policy. When a remote peer establishing a connection that matches this IKE policy, the particular CA profile or trusted CA group is used to validate the remote peer.

A group of trusted CA servers can be created with the trusted CA group configuration statement at the **[edit security pki]** hierarchy level; one or multiple CA profiles can be specified. The trusted CA server is bound to the IKE policy configuration for the peer at **[edit security ike policy policy certificate]** hierarchy level.

[See [Understanding Certificates and PKI](#) and [Understanding Certificate Authority Profiles](#).]

- **IPv6 support for AutoVPN and ADVPN with dynamic routing protocol (SRX Series and vSRX instances)**—Starting with Junos OS Release 18.1R1, IPv6 is supported on AutoVPN and Auto Discovery VPN (ADVPN) with point-to-multipoint secure tunnel mode. ADVPN can run with OSPFv3 routing protocol and AutoVPN can run with OSPFv3 and iBGP (internal BGP) routing protocols.

The **ospf3** option is introduced at the **edit protocol** hierarchy level to support IPv6 for AutoVPN and ADVPN with point-to-multipoint secure tunnel mode. In addition, the **show security ipsec next-hop-tunnels** command, which displays the IPsec VPN tunnels bound to a specific tunnel interface, is updated to add **family** and **tunnel ID** filters.

[See [Understanding AutoVPN](#) and [Understanding Auto Discovery VPN](#).]

- **IPv6 support for PKI (SRX Series and vSRX instances)**—Starting in Junos OS Release 18.1, the public key infrastructure (PKI) supports IPv6 address format for the Certificate Authority (CA) server and source addresses in a CA profile. The PKI provides an infrastructure for digital certificate management. In PKI, a CA is a trusted third party agency responsible for issuing and revoking certificates. The certificates are used to create secure connections between two or more entities.

[See [Understanding Certificate Authority Profiles](#).]

- **SSL remote access VPN support by bypassing an application-based firewall (SRX Series and vSRX instances)**—Starting with Junos OS Release 18.1R1, remote access VPN uses SSL to pass through an application level firewall using the third-party NCP Exclusive Remote Access Client on Windows, MAC OS, Apple iOS, and Android devices.

Most intermediate Internet-facing devices allow users to establish a session over SSL (HTTPS) to any Internet-based device. This solution allows users to establish a secure communication using a full SSL session when an intermediate device blocks IPsec or UDP traffic.

[See [Understanding SSL Remote Access VPNs with NCP Exclusive Remote Access Client](#).]

SEE ALSO

[Changes in Behavior and Syntax](#) | 271

[Known Behavior](#) | 272

[Known Issues](#) | 274

[Resolved Issues](#) | 276

[Documentation Updates](#) | 285

[Migration, Upgrade, and Downgrade Instructions](#) | 286

[Product Compatibility](#) | 287

Changes in Behavior and Syntax

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 18.1R2 for the SRX Series.

Chassis Cluster

- **IP Monitoring**—Starting with Junos OS Release 18.1R2, on all SRX Series devices, if the reth interface is in bundled state, IP monitoring for redundant groups is not supported on the secondary node. This is because the secondary node sends reply using the lowest port in the bundle which is having a different physical MAC address. The reply is not received on the same physical port from which the request is sent. If the reply comes on the other interface of the bundle, then the internal switch drops it.
- **Power Entry Module**—Starting with Junos OS Release 18.1R2, when you use DC PEM on SRX Series devices operating in chassis cluster mode, the output of **show chassis power** command shows **DC input: 48.0 V input (57000 mV)**. The value **48.0 V input** is a fixed string and can be interpreted as a measured input voltage. The acceptable range of DC input voltage accepted by the DC PEM is 40 to 72 V. The **(57500 mV)** is a measured value, but is not related with the input. It is the actual output value of the PEM and the value is variable. The **DC input:** from **show chassis power** and **Voltage:** information from **show chassis environment pem** command output are removed for each PEM.

IDP

- **Custom Attack (SRX Series)**—Starting with Junos OS Release 18.1R2, the maximum number of characters allowed for a custom attack object name is 60. You can validate the statement using the CLI **set security idp custom-attack** command.

SEE ALSO

[New and Changed Features | 265](#)

[Known Behavior | 272](#)

[Known Issues | 274](#)

[Resolved Issues | 276](#)

[Documentation Updates | 285](#)

[Migration, Upgrade, and Downgrade Instructions | 286](#)

[Product Compatibility | 287](#)

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 18.1R2 for the SRX Series.

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

Chassis Clustering

- On SRX4600 devices, the dedicated Chassis Cluster fabric ports are not available. Instead, any 40G or 10G traffic ports can be used as chassis cluster fabric ports.
- On SRX Series devices, in rare situations, the RG1+ failover might occur because of FPC or SPU failure which might trigger the MAC move protection on the neighboring switch. [PR1333505](#)
- On SRX300, SRX320, SRX340, SRX345, and SRX550 devices, if you enable IP monitoring on redundancy groups, the feature might not work correctly on the secondary node if the reth interface has more than one physical interfaces configured on each node, which enables an RLAG (Redundant Link Aggregation). This issue occurs because the backup node will send traffic using the MAC address of the lowest port in the bundle. If the response towards the same mac address arrives on a different physical port in the bundle, then the internal switch in the SRX device will drop the response packets. [PR1344173](#)

Interfaces and Chassis

- SRX4600 device interfaces only support the following two traffic port modes:
 - 4x40G (all four QSFP+ ports) + 8x10G (all eight SFP+ ports) by default.
 - 2x100G (first two QSFP+ ports) + 4x10G (first four SFP+ ports) by configuration as shown below:
 - **set chassis fpc 1 pic 0 pic-mode 100G**
 - **set chassis fpc 1 pic 0 number-of-ports 2**
 - **set chassis fpc 1 pic 1 number-of-ports 4**

NOTE: The system requires a reboot after committing the above configuration.

- On SRX4600 devices, the RAID-1 mirror feature is not available. The second SSD is not available for use, although it is present.
- On SRX4600 devices, precision Time Protocol (PTP) feature is not available.

J-Web

- On SRX Series devices, the DHCP relay configuration in J-Web under **Configure>Services>DHCP>DHCP Relay** page is not available. However, the same DHCP relay can be configured using the CLI. [PR1205911](#)
- On SRX Series devices, DHCP client bindings under Monitor page is removed. However the same bindings can be seen in the CLI by using the **show dhcp client binding** command. [PR1205915](#)
- On SRX Series devices, adding 2,000 global addresses at a time to a list of SSL proxy profile exempted addresses can cause the Web page to stop responding. [PR1278087](#)
- On SRX Series devices, you cannot view the custom log files created for event logging in the J-Web. [PR1280857](#)
- In the factory default configuration, the following commands to open up the Phone home page: **set system phone-home server https://redirect.juniper.net** and **set system phone-home rfc-complaint**. If you want to configure the device using J-Web click the **SKIP to JWEB** option. After clicking the SKIP to JWEB option, you will be asked for root authentication password and to clear the phone commands in CLI. The session will redirect to the J-Web page automatically to configure the Setup wizard. Automatic redirection does not work in FireFox or the Internet Explore. You need to perform a manual refresh in these browsers. [PR1284341](#)
- Validation is not checked when the UTM policy is detached from the firewall policy rule after an SSL proxy profile is selected. [PR1285543](#)
- Uploading certificates using the browse button stores the certificate at **/jail/var/tmp/uploads/**, which is deleted on running the **request system storage cleanup** command. [PR1312529](#)
- The values of **address** and **address-range** are not displayed in the inline **address-set** creation pop-up window of JIMS. [PR1312900](#)
- Application signature install or uninstall status above the grid remains in loading state when the device connectivity to the cloud server. Application signature database is not present or not responding. This in turn affects the status that is displayed in the J-Web. [PR1332768](#)

Platform and Infrastructure

- On SRX4600 devices, the USB flash drive is not available to Junos OS. However, the USB flash drive is available for the host OS (Linux) with full access. The USB flash drive is still used in the booting process (install and recovery functions). [PR1283618](#)
- When a USB device is under initialization, removing the USB device might cause the USB to stop working. [PR1332360](#)

Software Installation and Upgrade

- When you upgrade from Junos OS Release 15.1X49, the signature version is automatically refreshed to version 534. Hence, you need to download and install a new signature version; if not, some features such as SKYATP IMAP might be missing. [PR1324848](#)

User Interface and Configuration

- On SRX1500 devices, committing a configuration with a huge number of logical systems will take more time. This issue occurs because taking backup of previous configurations might take a little longer to finish. [PR1339862](#)

VPNs

- On SRX Series devices, IPsec traffic statistics counters return 32-bit values, which might quickly overflow. [PR1301688](#)
- On SRX5400, SRX5600, and SRX5800 devices, when CoS is enabled on the st0 interface and the incoming traffic rate destined for the st0 interface is higher than 300,000 packets per second (pps) per SPU, the device might drop some of the high-priority packets internally and shaping of outgoing traffic might be impacted. We recommended that you configure the appropriate policer on the ingress interface to limit the traffic below 300,000 pps per SPU. [PR1239021](#)

SEE ALSO

[New and Changed Features | 265](#)

[Changes in Behavior and Syntax | 271](#)

[Known Issues | 274](#)

[Resolved Issues | 276](#)

[Documentation Updates | 285](#)

[Migration, Upgrade, and Downgrade Instructions | 286](#)

[Product Compatibility | 287](#)

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 18.1R2 for SRX Series devices.

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

Chassis Clustering

- On SRX5600 and SRX5800 devices in chassis cluster mode, when the secondary Routing Engine is installed to enable dual control links, the **show chassis hardware** command might display the same serial number for both the routing engines on both the nodes. [PR1321502](#)
- On SRX Series devices, the forwarding plane might failover from node 0 to node 1 when an SPC stops unexpectedly. [PR1331809](#)

Class of Service (CoS)

- On all SRX Series devices, if the action of **forwarding-class** is configured in the output direction on a firewall filter, the host outbound traffic matching the same term of this firewall filter is blocked. [PR1272286](#)

Flow-Based and Packet-Based Processing

- On all SRX Series devices, filter-based forwarding (FBF) does not work when applied on IPsec tunnel interface (st0.*). [PR1290834](#)
- On SRX Series devices, when you run the command **clear nhdb statistics** on the SPU PIC, the SPC might reset. [PR1346320](#)

Intrusion Detection and Prevention (IDP)

- The output of **show security idp status** command does not accurately reflect the number of decrypted SSL or TLS sessions being inspected by the IDP. [PR1304666](#)
- The file descriptor might leak during a security package auto update. [PR1318727](#)

Software Installation and Upgrade

- On SRX1500 devices, the fan speed often fluctuates. [PR1335523](#)

VPNs

- When an SRX Series device acts as an initiator behind the NAT, disabling NAT on the router in between causes an immediate new negotiation failure because of an attempt to disable NAT using the port 4,500. The next attempt succeeds by using the port 500. Disabling NAT and bringing down all the existing tunnels and re-establishing the tunnels with port 500 is the expected behavior. [PR1273213](#)
- On SRX Series devices, in case multiple traffic-selectors are configured for a peer with IKEv2 reauthentication, only one traffic-selector rekeys at the time of IKEv2 reauthentication. The VPN tunnels of the remaining traffic-selectors are cleared without immediate rekey. New negotiation of those traffic-selectors might be triggered through other mechanisms such as traffic or peer. [PR1287168](#)
- When NCP profile is changed on an existing IKE gateway, the SSL session corresponding to the existing tunnel is not affected. [PR1323425](#)
- If a period . is present in the CA profile name then the PKID might face issues, if the PKID is restarted at any point. [PR1351727](#)

SEE ALSO

[New and Changed Features | 265](#)

[Changes in Behavior and Syntax | 271](#)

[Known Behavior | 272](#)

[Resolved Issues | 276](#)

[Documentation Updates | 285](#)

[Migration, Upgrade, and Downgrade Instructions | 286](#)

[Product Compatibility | 287](#)

Resolved Issues

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: 18.1R2

API

- On SRX320-POE devices, the REST API does not work when the relevant configuration is added under the **system services rest** hierarchy. [PR1347539](#)

Application Layer Gateways (ALGs)

- On SRX5400, SRX5600, and SRX5800 devices, when you use the SIP ALG and have multiple local SIP servers with consecutive IP addresses, the SIP session distribution over the SPUs might not be optimal. [PR1337549](#)

Authentication and Access Control

- The **uacd** process is not stable after upgrading to Junos OS Release 12.3X48 release. [PR1336356](#)
- On SRX Series devices, **show version detail** command displays the following error message: **Unrecognized command (user-ad-authentication)** when configuring the USERIDD. [PR1337740](#)
- New configuration is available to configure the **web-authentication** timeout. [PR1339627](#)

Chassis Clustering

- The FPC module is offline at the secondary node, after the primary node or the secondary node is restarted. [PR1340116](#)
- On SRX5400, SRX5600, and SRX5800 devices with DC PEM installed on the device, the output of **show chassis environment pem** and **show chassis power** commands do not accurately reflect the actual value. [PR1323256](#)
- IP monitoring is not working as expected when one node is in secondary-hold and the primary node priority becomes 0. [PR1330821](#)
- On SRX Series devices, the integrated routing and bridging (IRB) interface on high availability does not send the ARP request after clearing ARP. [PR1338445](#)
- When a PPPoE interface is configured over an Aggregate Ethernet (AE) or redundant ethernet (RETH) interfaces, reboot of the cluster nodes might occur in some cases. [PR1341968](#)

Class of Service (CoS)

- Packets are out-of-order on the SRX5K-SPC-4-15-320 card (SPC2) cards with IOC1 or FIOC cards. [PR1339551](#)

Flow-Based and Packet-Based Processing

- The forwarding plane drops the packets, when J-Flow version 9 related configuration is removed. [PR1351102](#)
- On SRX Series devices, packet reorder might occur in traffic when using Point-to-Point protocol (PPP). [PR1340417](#)

- The flowd process might stop when the SYN-proxy function is configured. [PR1343920](#)
- File download halts over a period of time when the TCP proxy is activated through antivirus or Sky ATP. [PR1349351](#)
- On SRX1500, SRX4100, and SRX4200 devices, if the Sky ATP cloud feeds updates, the packet forwarding engine might stop causing intermittent traffic loss. [PR1315642](#)

Intrusion Detection and Prevention (IDP)

- On SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices, if IDP and SSL forward proxy whitelist are used together, the device might generate a core file. [PR1314282](#)
- Unable to load IDP policy because of less available heap memory. [PR1347821](#)

J-Web

- Unable to delete the dynamic VPN user configuration using J-Web. [PR1348705](#)

Platform and Infrastructure

- SRX5400, SRX5600, and SRX5800 devices, the message **No Port is enabled for FPC# on node0** is observed in the chassis process (**chassisd**) log for every 5 seconds. [PR1335486](#)
- SRX1500 devices might encounter a failure while accessing the SSD drive. [PR1345275](#)
- On SRX300 devices, the **show system firmware** command displays old firmware image. [PR1345314](#)
- On SRX Series devices, mandatory argument is missing for **show usp policy counters** command in RSI. [PR1341042](#)
- Simultaneous commit triggers the configuration integrity check failure and halts the SRX. [PR1332605](#)

Routing Policy and Firewall Filters

- On SRX Series devices, if you configure a huge number of custom applications in the policies, the flowd process might stop. [PR1347822](#)
- The log messages **L2ALM Trying peer/master connection, status 26** is displayed on all SRX Series devices. [PR1317011](#)
- The flowd process stops when AppQoS is configured on the device. [PR1319051](#)

Routing Protocols

- When BGP traceoptions are configured and enabled, the traces specific to the messages sent to the BGP peer (BGP SEND traces) are not logged, but the traces specific to the received messages (BGP RECV traces) are logged correctly. [PR1318830](#)
- OpenSSL Security Advisory, refer to <https://kb.juniper.net/JSA10851> for more information. [PR1328891](#)

Software Installation and Upgrade

- On SRX Series devices, if power loss occurs few seconds after commit and if the Trusted Platform Module is enabled, the configuration integrity fails. [PR1351256](#).

VPNs

- For FIPS: PKID, the syslog for key-pair deletion is required for conformance. [PR1308364](#)
- The kmd process might generate a core file when all the VPNs are down. [PR1336368](#)

Resolved Issues: 18.1R1

Application Layer Gateways (ALGs)

- On SRX Series devices, SIP packets might drop when SIP traffic performs destination NAT. [PR1268767](#)
- H323 ALG does not work correctly with static NAT and VR. [PR1303575](#)
- H323 ALG decode Q931 packet error is observed even after H323 ALG is disabled. [PR1305598](#)
- HTTP ALG is listed within **show security match-policies**, when the HTTP ALG does not exist. [PR1308717](#)
- On SRX Series devices with SIP ALG enabled, the SIP ALG might drop SIP packets which have a "referred-by" or "referred-to header" field containing multiple header parameters. [PR1328266](#)
- When SIP ALG is enabled and NAT is used, cores might be observed and then the device might reboot after the cores. [PR1330254](#)

Authentication and Access Control

- PFE might stop working, resulting in generation of huge number of core files in a short period of time. [PR1326677](#)
- JIMS server stops responding to requests from SRX Series devices. [PR1311446](#)
- On SRX Series devices, incomplete RSI might be seen. [PR1329967](#)
- On SRX Series devices, sessions might be closed because of **idle Timeout junos-fwauth-adapter**. [PR1330926](#)

Chassis Clustering

- The ISSU or ICU operation might fail if the upgrade is initiated from Junos Space on multiple SRX clusters. [PR1279916](#)
- Warning messages are tagged with error tag wrongly in the RPC response from an SRX Series device when you configure a change through netconf. [PR1286903](#)
- On SRX Series devices, if you are running the User Firewall feature, under some condition, core files are seen with the flow process or user identification process. The Packet Forwarding Engine is restarted, and RG1+ failover occurs. [PR1299494](#)

- Flowd process core files are generated after adding 65536 VPN tunnels using traffic selector with the same remote IP. [PR1301928](#)
- ISSU might be unsuccessful if the control link recovery is configured. [PR1303948](#)
- On SRX1500, SRX4100 and SRX4200 devices, ISSU might fail if LACP and interface monitoring are configured. [PR1305471](#)
- File Descriptor might leak on SRX Series chassis clusters with Sky ATP enabled. [PR1306218](#)
- After the device is rebooted, IP monitoring on secondary node shows unknown status. [PR1307749](#)
- In and active/active cluster, route change timeout does not work as expected. [PR1314162](#)
- When ISSU is performed from a Junos OS Release prior to 15.1X49-D60 to a Junos OS Release 15.1X49-D60 or later, flowd process generates core files. [PR1320030](#)
- When RG0 failover or primary node reboot happens, some of the logical interfaces might not be synchronized to the other node if the system has around 2000 logical interfaces and 40,000 security policies. [PR1331070](#)
- The default-gateway route received by DHCP when some interface in the chassis cluster has been configured as a DHCP client is lost in about 3 minutes after RG0 failover. [PR1334016](#)

Flow-Based and Packet-Based Processing

- On SRX4100 and SRX4200 devices, packet loss is observed when the value of packet per second (pps) through the device is very high. This occurs due to the update of the **application interval statistics** statement, which has a default timer value of 1 minute. You can avoid this issue by setting the interval to maximum using the **set services application-identification statistics interval 1440** command. [PR1290945](#)
- If SDNS proxy is configured on SRX Series devices, the naming process might stop. [PR1307435](#)
- When executing operations for creating rescue configuration, some errors are reported but the rescue configuration is created. [PR1280976](#)
- RPM packets not account through LT interface under certain configurations. [PR1303445](#)
- Packet capture does not work after the value of the **maximum-capture-size** option is modified. [PR1304723](#)
- The **show host server name-server host** CLI command fails when the source address is specified under the name-server configuration. [PR1307128](#)
- Clear session takes 9 minutes to clear 57 million sessions. [PR1308901](#)
- On SRX Series devices, if destination NAT and session affinity are configured with multiple traffic selectors in IPsec VPN, the traffic selector match might fail. [PR1309565](#)
- The flow process might stop and generate a core file during failover between node 0 and node 1. [PR1311412](#)
- On SRX Series devices, the IPsec tunnel might fail to be established if datapath debug configuration include the options **preserve-trace-order**, **record-pic-history**, or both. [PR1311454](#)

- The SRX Series device drops packets citing the reason "Drop pak on auth policy, not authed". [PR1312676](#)
- When you commit configuration changes involving deletion of routing-instance with application-tracking and session-close log enabled for the zone a PFE core file is generated. [PR1312757](#)
- The flow process might stop if the SSL-FP profile is configured with whitelist. [PR1313451](#)
- On SRX550M devices, phone-home.core is generated after the zeroization procedure. [PR1315367](#)
- On SRX Series devices, the PIM register stop comes before the PIM register packet. The out-of-sequence packet causes the flow session build error. [PR1316428](#)
- On SRX Series devices, the **fin-invalidate-sessio** command does not work when the Express Path feature is enabled on the device. [PR1316833](#)
- Return traffic through the routing instance might drop intermittently after changing the zone and routing-instance configuration on the st0.x interface. [PR1316839](#)
- SRX300 devices DHCP client cannot obtain IP addresses. [PR1317197](#)
- Default route is lost after system zero. [PR1317630](#)
- SSL firewall proxy does not work if root-ca has fewer than four characters. [PR1319755](#)
- Software next-hop table is full with log messages RT_PFE: NH IPC op 1 (ADD NEXTHOP) failed, err 6 (No Memory) peer_class 0, peer_index 0 peer_type 10. [PR1326475](#)
- The FPC is dropped or gets stuck in present state when intermittent control link heartbeats are seen. [PR1329745](#)
- The OSPF peers are unable to establish neighbors between the LT interfaces of the logical systems. [PR1319859](#)
- Flow process generates core files on both nodes causing an outage. [PR1324476](#)
- On the SRX5000 line of devices with an SRX5K-MPC3-40G10G (IOC3) or an SRX5K-MPC3-100G10G, the IPv6 traffic might be dropped if the IOC3 with the service-offload (npcache) feature is applied. [PR1331401](#)
- Inaccurate Jflow records might be seen for output interface and next hop. [PR1332666](#)
- The whitelist function in syn-flood does not work. [PR1332902](#)

Interfaces and Chassis

- LLDP protocol is not supported on a reth interface but it can be configured. [PR1127960](#)
- Traffic is looped with MSTP for untag traffic from IxNetwork ports. [PR1259099](#)
- Unable to add IRB and aggregated Ethernet interfaces. [PR1310791](#)
- On SRX1500 devices, pp0.0 interface link status is not up. [PR1315416](#)

- An error is not seen at each commit or commit check if autonegotiation is disabled but the speed and duplex configurations are not configured on the interface. [PR1316965](#)
- RSI uses incorrect **show vlans** syntax. [PR1336267](#)

Intrusion Detection and Prevention (IDP)

- On SRX4600 devices, the maximum SSLRP session count is observed to be approaching 100,000. In the CLI, configuring a maximum of 100,000 sessions are allowed, whereas in SSLFP, 600,000 sessions are allowed. Thus, the **set security idp sensor-configuration ssl-inspection sessions** command is now modified to allow a maximum of 600, 000 sessions. However, for other devices the original session limit value of 100,000 is retained. [PR1329827](#)
- IDP policy compilation can be triggered even if changes that are not related to IDP are performed. [PR1283379](#)
- IDP signatures might not get pushed to the Packet Forwarding Engine if there is a policy in logical systems. [PR1298530](#)
- On SRX Series devices, IDP PCAP feature underwent improvements such as:
 - The first valid packet-log-id will no longer be generated as '0' as this was not compatible with third party tools.
 - The algorithm for assigning packet-log-id's is improved to reduce the likelihood of duplicate entries and id-rollover events, particularly among devices with multiple SPU's.

[PR1297876](#)

J-Web

- J-Web system snapshot throws error. [PR1204587](#)
- J-Web does not display all global address book entries. [PR1302307](#)
- J-Web removes backslash character on source identity object when committing changes. [PR1304608](#)
- In J-Web, the zone drop-down does not list the available zones while creating the zone address book or sets with Internet Explorer IE 10 or 11. [PR1308684](#)
- J-Web authentication fails when a password includes the backslash. [PR1316915](#)
- J-Web dashboard displays wrong last updated time. [PR1318006](#)
- J-Web display problems for security policies are observed. [PR1318118](#)
- J-Web does not display wizards on the dashboard. [PR1330283](#)

Layer 2 Ethernet Services

- Duplicate hops or more than expected hop count is seen in Layer 2 traceroute. [PR1243213](#)
- Ping to VRRP(VIP) address failed when VRRP is on VLAN tagging. It only affects Trio-based IOC2 and IOC3 in SRX5000 line of devices. Other devices are not affected. [PR1293808](#)

- DHCPv6 prefix delegation does not start with the first available subnet. [PR1295178](#)
- In DHCP relay configuration, the option **VPN** has been renamed to **source-ip-change**. [PR1318487](#)
- DHCP rebind and renew packets is not calculated in BOOTREQUEST. [PR1325872](#)

Network Address Translation (NAT)

- SCTP packet has incorrect SCTP checksum after the SRX Series device implements NAT on the payload. [PR1310141](#)
- Active source NAT causes an NSD error and the session closes. [PR1313144](#)
- On SRX340 and SRX345 devices, configuring the source NAT pool larger than 1024 fails. [PR1321480](#)
- Arena utilization on a FPC spikes and then resumes to a normal value. [PR1336228](#)

Network Security

- On SRX Series devices, the Sky ATP connection leak causes the service plane to be disconnected from the Sky ATP cloud. [PR1329238](#)

Network Management and Monitoring

- DHCP packets are dropped by the dot1x module, if the port is a multiple-suplicant port. [PR1296734](#)
- On SRX Series devices, the Routing Engine does not reply to an SNMP request. [PR1240178](#)
- SRX1500 devices might power-off unexpectedly because of incorrect device temperature readings, which reported very high temperature, leading to an immediate proactive powering -off of the device to protect the device from overheating. However, in these cases the temperature was not actually too high and a power-off would not be required. When this occurs, the following log message is shown in file `/var/log/hostlogs/lcmd.log`: `Jan 25 13:09:44 localhost lcmd[3561]: srx_shutdown:214: called with FRU TmpSensor`. [PR1241061](#)
- On SRX Series devices, when J-flow is enabled for multicast traffic, **extern nexthop** is installed during the multicast composite next hop. However, when you uninstall the composite next hop, it does not free the **extern nexthop**, which results in the jtree memory leak. [PR1276133](#)
- SRX300 device is unresponsive as a result of `cf/var: filesystem full` error. [PR1289489](#)
- CLI options are available to manage the packet forwarding engine handling the ARP throttling for NHDB resolutions. [PR1302384](#)

Platform and Infrastructure

- SRX Series devices do not process traffic because of an IPv6 NDP packets burst. [PR1293673](#)
- Inconsistent flow-control status on reth interfaces is observed. [PR1302293](#)
- On SRX5400, SRX5600, SRX5800 devices, SPC2 XLP stops processing packets in the ingress direction after repeated RSI collections. [PR1326584](#)

- On SRX5400, SRX5600, and SRX5800 devices, the packet captured by datapath-debug on an IOC2 card might be truncated. [PR1300351](#)
- When Security Intelligence (SecIntel) is configured, IPFD CPU utilization might be higher than expected. [PR1326644](#)

Routing Policy and Firewall Filters

- BGP traceoption logs are written even when it is deactivated. [PR1307690](#)
- The nsd process might stop responding when the name of a logical system is replaced. [PR1307876](#)
- The number of address objects per policy for SRX5400, SRX5600, SRX5800 devices is increased from 4096 to 16,000. [PR1315625](#)

Routing Protocols

- On SRX1500 devices, the IS-IS adjacency remains down when using an IRB interface. [PR1300743](#)
- Dedicated BFD does not work on SRX Series devices. [PR1312298](#)
- In a chassis cluster device with BMP configured, the rpd process might stop responding when the rpd process gracefully terminates. [PR1315798](#)

Software Installation and Upgrade

- The **request system reboot node in/at** command results in an immediate reboot instead of rebooting at the allotted time. [PR1303686](#)

Unified Threat Management (UTM)

- On SRX series, if Sophos antispam or Sophos antivirus interfaces are in a routing-instance, the feature might not work as expected. [PR1311694](#)
- The ISSU upgrade might fail because of the generation of Packet Forwarding Engine core files. [PR1328665](#)

VPNs

- The IRB interface does not support VPN. [PR1166714](#)
- Output hangs while checking pki ca-certificate ca-profile-group details. [PR1276619](#)
- Next hop tunnel binding (NHTB) is not installed occasionally during rekey for VPN using IKEv1. [PR1281833](#)
- Traffic through tunnel fails without configuring th authentication algorithm under IPsec proposal on SRX1500 devices. SRX5600 it works correctly. [PR1285284](#)
- ADVPN tunnels flap with spoke error **no response ready yet**, this issue leads to IKEv2 timeout. [PR1305451](#)
- On SRX Series devices, core files are observed under certain conditions with VPN and when NAT-T is enabled. [PR1308072](#)
- SNMP for jnxIpSecTunMonVpnName does not work. [PR1330365](#)

- The kmd process core files might be seen when all the VPNs are down. [PR1336368](#)
- On SRX Series devices, ESP packet drops in IPsec VPN tunnels with NULL encryption algorithm configuration are observed. [PR1329368](#)

SEE ALSO

[New and Changed Features | 265](#)

[Changes in Behavior and Syntax | 271](#)

[Known Behavior | 272](#)

[Known Issues | 274](#)

[Documentation Updates | 285](#)

[Migration, Upgrade, and Downgrade Instructions | 286](#)

[Product Compatibility | 287](#)

Documentation Updates

IN THIS SECTION

- [New Simplified Documentation Architecture | 285](#)

This section lists the errata and changes in Junos OS Release 18.1R1 for the SRX Series device documentation.

New Simplified Documentation Architecture

- With the release of Junos OS Release 18.1, Juniper is simplifying its technical documentation to make it easier for you to find information and know that you can rely on it when you find it. In the past, we organized documentation about Junos OS software features into platform-specific documents. In many cases, features are supported on multiple platforms, so you might not easily find the document you want for your platform.

With Junos OS Release 18.1, we have eliminated the platform-specific software feature documents. For example, if you want to find documentation on OSPF, there is only one document regardless of which platform you have. Here are some of the benefits of our new simplified architecture:

- Over time, you will see better search results when looking for Juniper documentation. You will be able to find what you want faster and be assured that is the right document.
- If a software feature is supported on multiple platforms, you can find information about all the platforms in one place.
- Because we have eliminated many documents that covered similar topics, you will now find one document with all the information.
- You can know that you are always getting the most current and accurate information.

SEE ALSO

[New and Changed Features | 265](#)

[Changes in Behavior and Syntax | 271](#)

[Known Behavior | 272](#)

[Known Issues | 274](#)

[Resolved Issues | 276](#)

[Migration, Upgrade, and Downgrade Instructions | 286](#)

[Product Compatibility | 287](#)

Migration, Upgrade, and Downgrade Instructions

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 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 Releases 12.3X48, 15.1X49, 17.3, and 17.4 are EEOL releases. You can upgrade from Junos OS Release 15.1X49 to Release 17.3 or from Junos OS Release 15.1X49 to Release 17.4.

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

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

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 | 265](#)

[Changes in Behavior and Syntax | 271](#)

[Known Behavior | 272](#)

[Known Issues | 274](#)

[Resolved Issues | 276](#)

[Documentation Updates | 285](#)

[Product Compatibility | 287](#)

Product 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 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

New and Changed Features	265
Changes in Behavior and Syntax	271
Known Behavior	272
Known Issues	274
Resolved Issues	276
Documentation Updates	285
Migration, Upgrade, and Downgrade Instructions	286

Third-Party Components

This product includes third-party components. To obtain a complete list of third-party components, see [Copyright and Trademark Information](#).

Upgrading Using ISSU

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.

For additional information about using ISSU on Routing and Switching devices, see the [High Availability User Guide](#)

For additional information about using ISSU on Security devices, see the [Chassis Cluster User Guide for SRX Series 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 the Junos OS, see the Juniper Networks Problem Report Search application at <https://prsearch.juniper.net>.

For regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

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/>.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at

<https://www.juniper.net/documentation/content-applications/content-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 rating system—On any page at the Juniper Networks Technical Documentation site at <https://www.juniper.net/documentation/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/documentation/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://www.juniper.net/support/warranty/>.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- 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/> .

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://www.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/cgi-bin/docbugreport/>.

Revision History

26 August 2021—Revision 12, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

31 October 2019—Revision 11, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

24 October 2019—Revision 10, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

7 March 2019—Revision 9, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

29 November 2018—Revision 8, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

14 September 2018—Revision 7, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

14 August 2018—Revision 6, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

3 August 2018—Revision 5, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

12 July 2018—Revision 4, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

28 June 2018—Revision 3, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

8 June 2018—Revision 2, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

1 June 2018—Revision 1, Junos OS Release 18.1R2— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

26 April 2018—Revision 6, Junos OS Release 18.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

19 April 2018—Revision 5, Junos OS Release 18.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

10 April 2018—Revision 4, Junos OS Release 18.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

6 April 2018—Revision 3, Junos OS Release 18.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

3 April 2018—Revision 2, Junos OS Release 18.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

27 March 2018—Revision 1, Junos OS Release 18.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

Copyright © 2018 Juniper Networks, Inc. All rights reserved.

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.