

Release Notes

Published
2021-09-30

Junos[®] OS 17.3R1 Release Notes

SUPPORTED ON

- ACX Series, EX Series, Junos Fusion Enterprise, Junos Fusion Data Center, Junos Fusion Provider Edge, MX Series, PTX Series, QFX Series, and SRX Series

HARDWARE HIGHLIGHTS

- Support for 100 MB Optics (ACX Series)
- Support for MPCs, PICs, and MICs (MX10003)

SOFTWARE HIGHLIGHTS

- Support for limiting the number of MAC entries for a logical interface (ACX5000)
- Support for hierarchical CoS for queues and schedulers (ACX5000)
- Support for IPv6 for RADIUS AAA (EX4300 and EX9200)
- Support for port bounce with CoA requests and Framed-IPv6-Address RADIUS attribute (EX4300 and EX9200)
- Support for two-way active measurement protocol (TWAMP) (EX4300)
- Support for VRRP scale improvements per aggregated Ethernet bundle (MX Series)
- Support for FRU control, power management and environmental monitoring (MX10003)
- Support for fabric management (MX10003)
- Support for inline flow monitoring (MX10003 router MPCs)
- Support for Junos Fusion Provider Edge (MX10003)

- Support for ping utility for testing CE device connectivity (MX Series with MPC and MIC)
- Support for secure boot (MX10003)
- Support for IPv6 GRE tunnels (MX Series)
- Support for Junos node slicing (MX480)
- Support for advanced forwarding interface (AFI) API (vMX routers)
- Support for Junos telemetry interface (PTX1000)
- Support for inline jflow version 9 flow templates (PTX1000)
- Support for increased number of aggregated Ethernet interfaces (QFX10008 and QFX10016)
- Security features delivered in Junos OS for SRX Series “X” releases from 12.1X44 through 15.1X49-D75
- Support for maximum number of security policies increased (SRX5400, SRX5600, SRX5800)
- Support for FreeBSD version 10 for Junos OS (SRX5800, SRX5600, SRX5400)

Release Notes: Junos[®] OS Release 17.3R1 for the ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion Junos OS 17.3R1 Release Notes

30 September 2021

Contents	Introduction 13
	Junos OS Release Notes for ACX Series 13
	New and Changed Features 14
	Hardware 14
	Class of Service 14
	Interfaces and Chassis 14
	Timing and Synchronization 15
	Changes in Behavior and Syntax 16
	General Routing 16
	Interfaces and Chassis 16
	Known Behavior 17
	Known Issues 17
	Hierarchical Class of Service 18
	Class of Service 18
	Layer 2 Features 18
	Router 18
	Resolved Issues 19
	Resolved Issues: 17.3R1 19
	Documentation Updates 20

Migration, Upgrade, and Downgrade Instructions | 20

Upgrade and Downgrade Support Policy for Junos OS Releases | 20

Product Compatibility | 21

Hardware Compatibility | 21

Junos OS Release Notes for EX Series Switches | 22

New and Changed Features | 23

Authentication, Authorization, and Accounting (AAA) (RADIUS) | 24

EVPNs | 25

Layer 2 Features | 26

Layer 3 Features | 26

Management | 27

Multiprotocol Label Switching (MPLS) | 29

Operation, Administration, and Maintenance | 29

Services Applications | 29

Changes in Behavior and Syntax | 30

General Routing | 30

Management | 30

Network Management and Monitoring | 31

VLAN Infrastructure | 31

Known Behavior | 31

Authentication, Authorization, and Accounting (AAA) (RADIUS) | 32

High Availability (HA) and Resiliency | 32

Known Issues | 33

Platform and Infrastructure | 33

Port Security | 33

User Interface and Configuration | 33

Resolved Issues | 34

Authentication, Authorization, and Accounting (AAA) (RADIUS) | 35

Infrastructure | 35

Layer 2 Features | 35

Platform and Infrastructure | 35

Documentation Updates | 35

Traffic Management User Guide for EX4600 Switches | 36

Migration, Upgrade, and Downgrade Instructions | 36

Upgrade and Downgrade Support Policy for Junos OS Releases | 37

Product Compatibility | 37

Hardware Compatibility | 38

Junos OS Release Notes for Junos Fusion Data Center | 38

New and Changed Features | 39

Changes in Behavior and Syntax | 39

Known Behavior | 40

Junos Fusion Data Center | 40

Known Issues | 41

Resolved Issues | 41

Documentation Updates | 42

Migration, Upgrade, and Downgrade Instructions | 42

Basic Procedure for Upgrading an Aggregation Device | 43

Preparing the Switch for Satellite Device Conversion | 45

Autoconverting a Switch into a Satellite Device | 47

Manually Converting a Switch into a Satellite Device | 50

Configuring a Switch into a Satellite Device Before Connecting It to a Junos Fusion
Topology | 52

Configuring Satellite Device Upgrade Groups | 53

Upgrade and Downgrade Support Policy for Junos OS Releases | 55

Downgrading from Release 17.3R1 | 55

Product Compatibility | 56

Hardware Compatibility | 56

Junos OS Release Notes for Junos Fusion Enterprise | 57

New and Changed Features | 57

Junos Fusion Enterprise | 58

Changes in Behavior and Syntax | 59

Junos Fusion Enterprise | 59

Known Behavior | 59

Junos Fusion Enterprise | 60

Known Issues | 60

Junos Fusion Enterprise | 61

Resolved Issues | 61**Resolved Issues: 17.3R1 | 62****Documentation Updates | 62****Migration, Upgrade, and Downgrade Instructions | 63****Basic Procedure for Upgrading Junos OS on an Aggregation Device | 63****Upgrading an Aggregation Device with Redundant Routing Engines | 66****Preparing the Switch for Satellite Device Conversion | 66****Converting a Satellite Device to a Standalone Switch | 67****Upgrade and Downgrade Support Policy for Junos OS Releases | 69****Downgrading from Release 17.3 | 70****Product Compatibility | 71****Hardware and Software Compatibility | 71****Hardware Compatibility Tool | 71****Junos OS Release Notes for Junos Fusion Provider Edge | 72****New and Changed Features | 72****Junos Fusion | 73****Changes in Behavior and Syntax | 74****Known Behavior | 74****Known Issues | 75****Resolved Issues | 75****Documentation Updates | 76****Migration, Upgrade, and Downgrade Instructions | 76****Basic Procedure for Upgrading an Aggregation Device | 77****Upgrading an Aggregation Device with Redundant Routing Engines | 79****Preparing the Switch for Satellite Device Conversion | 79****Converting a Satellite Device to a Standalone Device | 81****Upgrading an Aggregation Device | 83****Upgrade and Downgrade Support Policy for Junos OS Releases | 83****Downgrading from Release 17.3 | 83****Product Compatibility | 84****Hardware Compatibility | 84**

Junos OS Release Notes for MX Series 5G Universal Routing Platforms | 85

New and Changed Features | 86

Class of Service (CoS)	87
Dynamic Host Configuration Protocol (DHCP)	87
EVPNs	88
General Routing	90
High Availability (HA) and Resiliency	90
Interfaces and Chassis	91
IPSec	93
IPv6	93
Layer 2 Features	93
Layer 2 VPN	94
Layer 3 Features	95
Management	95
MPLS	96
Multicast	97
Network Management and Monitoring	98
Operation, Administration, and Maintenance (OAM)	98
Port Security	100
Routing Policy and Firewall Filters	100
Routing Protocols	101
Security	103
Services Applications	103
Software Defined Networking (SDN)	105
Subscriber Management and Services	105
Virtual Chassis	110

Changes in Behavior and Syntax | 110

EVPNs	111
General Routing	111
Interfaces and Chassis	111
Management	111
Network Management and Monitoring	112
Routing Protocols	113
Services Application	113

Subscriber Management and Services	113
VLAN Infrastructure	114
Known Behavior	115
General Routing	115
High Availability (HA) and Resiliency	115
Known Issues	116
Forwarding and Sampling	116
General Routing	117
Hardware	120
Infrastructure	120
Interfaces and Chassis	121
Layer 2 Features	121
MPLS	121
Platform and Infrastructure	122
Routing Protocols	122
Services Applications	122
VPN	122
Resolved Issues	123
Resolved Issues: 17.3R1	123
Documentation Updates	128
Subscriber Management Provisioning Guide	129
Migration, Upgrade, and Downgrade Instructions	129
Basic Procedure for Upgrading to Release 17.3	130
Procedure to Upgrade to FreeBSD 10.x based Junos OS	131
Procedure to Upgrade to FreeBSD 6.x based Junos OS	133
Upgrade and Downgrade Support Policy for Junos OS Releases	134
Upgrading a Router with Redundant Routing Engines	135
Downgrading from Release 17.3	135
Product Compatibility	136
Hardware Compatibility	136
Junos OS Release Notes for NFX Series	137
New and Changed Features	137
Juniper Device Manager	138
Changes in Behavior and Syntax	138

Known Behavior | 139

Known Issues | 139

Resolved Issues | 140

Documentation Updates | 140

Migration, Upgrade, and Downgrade Instructions | 141

 Upgrade and Downgrade Support Policy for Junos OS Releases | 141

Product Compatibility | 142

 Hardware Compatibility | 142

Junos OS Release Notes for PTX Series Packet Transport Routers | 143

New and Changed Features | 143

 Class of Service | 144

 General Routing | 145

 Interfaces and Chassis | 145

 Management | 146

 Multicast | 147

 Network Management and Monitoring | 148

 Operation, Administration, and Maintenance | 148

 Routing Policy and Firewall Filters | 149

 Routing Protocols | 150

 Services Applications | 151

Changes in Behavior and Syntax | 151

 Forwarding and Sampling | 152

 General Routing | 152

 Interfaces and Chassis | 152

 Management | 152

 Network Management and Monitoring | 153

 Services Application | 153

 VLAN-Infrastructure | 154

Known Behavior | 154

Known Issues | 155

 General Routing | 155

 Infrastructure | 156

 Interfaces and Chassis | 156

 Platform and Infrastructure | 156

Routing Protocols	156
Resolved Issues	157
Resolved Issues: 17.3R1	157
Documentation Updates	158
Migration, Upgrade, and Downgrade Instructions	158
Upgrade and Downgrade Support Policy for Junos OS Releases	158
Upgrading a Router with Redundant Routing Engines	159
Basic Procedure for Upgrading to Release 17.3	159
Product Compatibility	163
Hardware Compatibility	163
Junos OS Release Notes for the QFX Series	164
New and Changed Features	164
Class of Service (CoS)	166
EVPNs	166
General Routing	168
High Availability (HA) and Resiliency	168
Interfaces and Chassis	168
Layer 2 Features	170
Management	170
Multicast	173
Multiprotocol Label Switching (MPLS)	173
Network Management and Monitoring	174
Operation, Administration, and Maintenance	174
Port Security	174
Routing Protocols Policy and Firewall Filters	175
Routing Protocols	175
Virtual Chassis	178
Changes in Behavior and Syntax	179
General Routing	180
Management	180
Network Management and Monitoring	181
VLAN Infrastructure	181

Known Behavior | 181

- EVPNs | 182
- High Availability (HA) and Resiliency | 182
- Infrastructure | 182
- Interfaces and Chassis | 182
- Layer 2 Features | 182
- Routing Protocols | 183

Known Issues | 183

- EVPNs | 184
- Interfaces and Chassis | 184
- IPsec | 186
- Multiprotocol Label Switching (MPLS) | 186
- Routing Protocols | 186
- System Management | 186
- VLAN Infrastructure | 186

Resolved Issues | 187

- General Routing | 187
- Interfaces and Chassis | 187
- Layer 2 Features | 188
- Port Security | 188
- Routing Protocols | 188
- System Management | 188
- VXLAN | 188

Documentation Updates | 189

- Traffic Management User Guide for the QFX Series | 189

Migration, Upgrade, and Downgrade Instructions | 190

- Upgrading Software on QFX Series Switches | 190
- Installing the Software on QFX10002 Switches | 193
- 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 | 193
- Installing the Software on QFX10008 and QFX10016 Switches | 195
- Performing a Unified ISSU | 199
- Preparing the Switch for Software Installation | 200
- Upgrading the Software Using Unified ISSU | 200

Product Compatibility | 203

Hardware Compatibility | 203

Junos OS Release Notes for SRX Series | 204

New and Changed Features | 204

Flow and Processing | 205

IDP | 206

Interfaces and Chassis | 207

Junos OS XML API and Scripting | 207

Layer 2 Features | 207

Management | 208

Network Security | 208

Software Installation and Upgrade | 208

User Interface and Configuration | 209

Changes in Behavior and Syntax | 210

ALGs | 211

Access and User Management | 211

Application Security | 211

Authentication, Authorization and Accounting (AAA) | 211

Chassis Cluster | 211

CLI | 212

Dynamic Host Configuration Protocol (DHCP) | 212

Flow-based and Packet-based Processing | 213

General Packet Radio Service (GPRS) | 213

IDP | 214

J-Web | 214

Layer 2 Features | 214

NAT | 214

Network Management and Monitoring | 215

System Logs | 215

Unified Threat Management (UTM) | 215

VLAN Infrastructure | 216

Known Behavior | 216

Attack Detection and Prevention (ADP) | 217

Class of Service | 217

Flow-based and Packet-based Processing	218
General Packet Radio Service (GPRS)	218
Layer 2 Features	219
Multicast	219
Platform and Infrastructure	220
Software Installation and Upgrade	220
USB autoinstallation	221
VPN	221
Known Issues	222
Authentication and Access Control	222
CLI	223
Flow-based and Packet-based Processing	223
Interfaces and Chassis	223
J-Web	224
Layer 2 Ethernet Services	224
Platform and Infrastructure	224
VPNs	224
Resolved Issues	225
Interfaces and Chassis	226
Layer 2 Ethernet Services	226
Platform and Infrastructure	226
Routing Policy and Firewall Filters	226
Unified Threat Management (UTM)	226
VPNs	226
Documentation Updates	227
Migration, Upgrade, and Downgrade Instructions	227
Upgrade for Layer 2 Configuration	228
Upgrade and Downgrade Scripts for Address Book Configuration	228
Product Compatibility	231
Hardware Compatibility	231
Upgrading Using Unified ISSU	232
Compliance Advisor	232
Finding More Information	232
Documentation Feedback	232

Requesting Technical Support | 234

Self-Help Online Tools and Resources | 234

Opening a Case with JTAC | 235

Revision History | 235

Introduction

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

These release notes accompany Junos OS Release 17.3R1 for the ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Junos OS Release Notes for ACX Series

IN THIS SECTION

- New and Changed Features | 14
- Changes in Behavior and Syntax | 16
- Known Behavior | 17
- Known Issues | 17
- Resolved Issues | 19
- Documentation Updates | 20
- Migration, Upgrade, and Downgrade Instructions | 20
- Product Compatibility | 21

These release notes accompany Junos OS Release 17.3R1 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- [Hardware | 14](#)
- [Class of Service | 14](#)
- [Interfaces and Chassis | 14](#)
- [Timing and Synchronization | 15](#)

This section describes the new features or enhancements to existing features in Junos OS Release 17.3R1 for ACX Series Universal Metro Routers.

Hardware

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

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

Class of Service

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

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

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

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

Interfaces and Chassis

- **Support for limiting the number of MAC addresses learned from a logical interface (ACX5000)**—Starting in Junos OS Release 17.3R1, you can limit the number of MAC addresses learned from a logical interface

on the ACX5000 line of routers. The number of MAC entries learned on a logical interface can be limited by configuring a value for **interface-mac-limit**. The logical interface MAC limit allows the MAC address table space to be distributed among the different logical interfaces. The MAC limiting can be done for both VPLS and VLAN networks. The limits for a bridge domain and logical port can also be configured at the same time.

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

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

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

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

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

Timing and Synchronization

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

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

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

SEE ALSO

[Changes in Behavior and Syntax](#) | 16

[Known Behavior](#) | 17

[Documentation Updates](#) | 20

[Known Issues](#) | 17

[Resolved Issues](#) | 19

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

[Product Compatibility](#) | 21

Changes in Behavior and Syntax

IN THIS SECTION

- [General Routing | 16](#)
- [Interfaces and Chassis | 16](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 17.3R1 for the ACX Series.

General Routing

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

Interfaces and Chassis

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

SEE ALSO

New and Changed Features 14
Known Behavior 17
Documentation Updates 20
Known Issues 17
Resolved Issues 19
Migration, Upgrade, and Downgrade Instructions 20
Product Compatibility 21

Known Behavior

There are no known limitations in Junos OS Release 17.3R1 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	 14
Changes in Behavior and Syntax	 16
Documentation Updates	 20
Known Issues	 17
Resolved Issues	 19
Migration, Upgrade, and Downgrade Instructions	 20
Product Compatibility	 21

Known Issues

IN THIS SECTION

- [Hierarchical Class of Service](#) | [18](#)
- [Class of Service](#) | [18](#)
- [Layer 2 Features](#) | [18](#)
- [Router](#) | [18](#)

This section lists the known issues in hardware and software in Junos OS Release 17.3R1 for the ACX Series Universal Metro Routers.

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

Hierarchical Class of Service

- On ACX5000 line of routers, whenever you make a change to the queue modes and for the changes to take effect you will need to restart the PFE. [PR1256465](#)
- On ACX5000 line of routers, the **show class-of-service scheduler-hierarchy** CLI command is not supported. [PR1261835](#)
- On ACX5000 line of routers, the **show class-of-service interfaces queue *logical-interface-name*** CLI command does not show **Queue Buffer Usage** for a logical interface. As a workaround, you can use the PFE shell **show cos halp mmu buffer ifl** command to see the **Queue Buffer Usage** for a logical interface. [PR1272822](#)
- On ACX5000 line of routers, the **shared-buffer maximum** CLI statement for logical interface hierarchical class of service queues does not work correctly. [PR1275796](#)

Class of Service

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

Layer 2 Features

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

Router

- On ACX500 line of routers, performance issues are seen on the ACX500 Indoor AC router. [PR1290278](#)

SEE ALSO

[New and Changed Features | 14](#)

[Changes in Behavior and Syntax | 16](#)

[Known Behavior | 17](#)

[Documentation Updates | 20](#)

[Resolved Issues | 19](#)[Migration, Upgrade, and Downgrade Instructions | 20](#)[Product Compatibility | 21](#)

Resolved Issues

IN THIS SECTION

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

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

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

Resolved Issues: 17.3R1

Layer 2 Features

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

SEE ALSO

[New and Changed Features | 14](#)[Changes in Behavior and Syntax | 16](#)[Known Behavior | 17](#)[Documentation Updates | 20](#)[Known Issues | 17](#)[Migration, Upgrade, and Downgrade Instructions | 20](#)[Product Compatibility | 21](#)

Documentation Updates

There are no errata or changes in Junos OS Release 17.3R1 for the ACX Series documentation.

SEE ALSO

[New and Changed Features | 14](#)

[Changes in Behavior and Syntax | 16](#)

[Known Behavior | 17](#)

[Known Issues | 17](#)

[Resolved Issues | 19](#)

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

[Product Compatibility | 21](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 20](#)

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 14.1,

14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

For more information about EEOL releases and to review a list of EEOL releases, see <https://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 | 14](#)

[Changes in Behavior and Syntax | 16](#)

[Known Behavior | 17](#)

[Documentation Updates | 20](#)

[Known Issues | 17](#)

[Resolved Issues | 19](#)

[Product Compatibility | 21](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 21](#)

Hardware Compatibility

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

To determine the features supported on ACX Series routers in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature

information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://pathfinder.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

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

SEE ALSO

New and Changed Features 14
Changes in Behavior and Syntax 16
Known Behavior 17
Documentation Updates 20
Known Issues 17
Resolved Issues 19
Migration, Upgrade, and Downgrade Instructions 20

Junos OS Release Notes for EX Series Switches

IN THIS SECTION

- [New and Changed Features | 23](#)
- [Changes in Behavior and Syntax | 30](#)
- [Known Behavior | 31](#)
- [Known Issues | 33](#)
- [Resolved Issues | 34](#)
- [Documentation Updates | 35](#)
- [Migration, Upgrade, and Downgrade Instructions | 36](#)
- [Product Compatibility | 37](#)

These release notes accompany Junos OS Release 17.3R1 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- Authentication, Authorization, and Accounting (AAA) (RADIUS) | 24
- EVPNs | 25
- Layer 2 Features | 26
- Layer 3 Features | 26
- Management | 27
- Multiprotocol Label Switching (MPLS) | 29
- Operation, Administration, and Maintenance | 29
- Services Applications | 29

This section describes the new features and enhancements to existing features in Junos OS Release 17.3R1 for the EX Series.

NOTE: The following EX Series switches are supported in Junos OS Release 17.3R1: EX4300, EX4600, and EX9200.

NOTE: In Junos OS Release 17.3R1, J-Web is supported on the EX4300 and EX4600 switches in both standalone and Virtual Chassis setup.

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

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

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

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

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

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

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

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

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

EVPNs

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

On EX9200 switches, two models are supported:

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

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

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

- **IPv6 support over IRB interfaces for EVPN (EX9200 switches)**—Starting in Junos OS Release 17.3R1, the Ethernet VPN (EVPN) integrated routing and bridging (IRB) solution supports IPv6 and the Neighborhood Discovery Protocol (NDP). NDP is used by IPv6 nodes on the same link to discover each other's presence, determine each other's Link Layer addresses, find routers, and maintain reachability information about the paths to active neighbors. IPv6 addresses over IRB for EVPN is supported for unique VLAN EVPN instances and for virtual switches with protocol EVPN instances.

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

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

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

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

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

Layer 2 Features

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

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

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

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

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

[See [Understanding Layer 2 Protocol Tunneling on EX Series Switches.](#)]

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

[See [Understanding Layer 2 Protocol Tunneling on EX Series Switches.](#)]

Layer 3 Features

- **Port-based LAN broadcast traffic forwarding (port helpers) for multiple destination servers (EX9200)**—Starting in Junos OS Release 17.3R1, you can configure port helpers on EX9200 switches

with multiple destination servers for a given port. Port helpers listen on configured UDP ports for incoming LAN broadcast traffic, and forward those packets to configured destination servers as unicast traffic. Configure port helpers to listen on a port and forward the traffic to a specified server using the **forwarding-options helpers port *port-number*** configuration statement with one of the following options:

- Global—Specify only **server *server-ip-address*** to listen on *any* interface for the configured port.
- VLAN-specific—Specify **interface *irb-interface-name* server *server-ip-address*** to listen only on a specified IRB interface.
- Interface-specific—Specify **interface *l3-interface-name* server *server-ip-address*** to listen only on a specified Layer 3 interface.

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

Management

- **Support for the Junos Telemetry Interface (EX9200 switches)**—Starting with Junos OS Release 17.3R1, the Junos Telemetry Interface is supported on EX9200 switches. Both UDP and gRPC streaming of statistics are supported. Junos Telemetry Interface enables you to provision sensors to export telemetry data for various network elements without involving polling. The following sensors are supported on EX9200 switches:
 - Aggregated Ethernet interfaces configured with the Link Aggregation Control Protocol (gRPC streaming only)
 - Ethernet interfaces enabled with the Link Layer Discovery Protocol (gRPC streaming only)
 - RSVP interface events (gRPC streaming only)
 - BGP peers (gRPC streaming only)
 - Memory utilization for routing protocol tasks (gRPC streaming only)
 - LSP events and properties (gRPC streaming only)
 - LSP statistics (UDP and gRPC streaming)
 - Network Discovery Protocol table state (gRPC streaming only)
 - Address Resolution Protocol table state (gRPC streaming only)
 - IPFIX inline flow sampling (UDP streaming only)
 - Queue depth statistics for ingress and egress queue traffic (UDP streaming only)
 - Logical interfaces (UDP and gRPC streaming)
 - Firewall filter statistics (UDP and gRPC streaming)
 - Optical interfaces (UDP and gRPC streaming)
 - Network processing unit (NPU) memory (UDP and gRPC streaming)

- NPU memory utilization (UDP and gRPC streaming)
- CPU memory (UDP and gRPC streaming)
- Fabric statistics (UDP streaming only)
- Physical interfaces (UDP and gRPC streaming)
- Chassis components (gRPC streaming only)

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

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

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

The following sensors are supported:

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

To provision sensors to stream data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters for a specified list of OpenConfig commands paths. You must download the Junos Network Agent software package, which provides the interfaces to manage gRPC subscriptions. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models.

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

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

You can configure TWAMP to start or stop all of the sessions for all of the TWAMP clients, or start or stop a session for a specific TWAMP client. When you start all the test session configured for a particular

TWAMP client, the control-client initiates all requested testing with a Start-Sessions message, and the server sends an acknowledgment. If the control connection is not active between the server and the client, the control connection is also established and the test connections are started later. If the control-client name is not specified, all the configured test sessions are commenced.

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

Multiprotocol Label Switching (MPLS)

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

[See [RSVP Overview](#) .]

Operation, Administration, and Maintenance

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

Services Applications

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

SEE ALSO

[Changes in Behavior and Syntax](#) | 30

[Known Behavior](#) | 31

[Known Issues](#) | 33

[Resolved Issues | 34](#)

[Documentation Updates | 35](#)

[Migration, Upgrade, and Downgrade Instructions | 36](#)

[Product Compatibility | 37](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [General Routing | 30](#)
- [Management | 30](#)
- [Network Management and Monitoring | 31](#)
- [VLAN Infrastructure | 31](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 17.3R1 for the EX Series.

General Routing

- **Support for deletion of static routes when the BFD session goes down (EX Series)**—Starting with Junos OS Release 17.3R1, the default behavior of the static route at the `[edit routing-options static static-route bfd-admin-down]` hierarchy level is active. So, the static routes are deleted when the BFD receives a session down message. [See [Enabling BFD on Qualified Next Hops in Static Routes for Route Selection.](#)]

Management

- **Changes to custom YANG RPC syntax (EX Series)**—Starting in Junos OS Release 17.3, custom YANG RPCs have the following changes in syntax:
 - The `junos:action-execute` statement is a substatement to `junos:command`. In earlier releases, the `action-execute` and `command` statements are placed at the same level, and the `command` statement is optional.
 - The CLI formatting for a custom RPC is defined within the `junos-odl:format` statement, which takes an identifier as an argument. In earlier releases, the CLI formatting is defined using a container that includes the `junos-odl:cli-format` statement with no identifier.

- The **junos-odl:style** statement defines the formatting for different styles within the statement. In earlier releases, the CLI formatting for different styles is defined using a container that includes the **junos-odl:cli-format** and **junos-odl:style** statements.

Network Management and Monitoring

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

VLAN Infrastructure

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

SEE ALSO

New and Changed Features	 23
Known Behavior	 31
Known Issues	 33
Resolved Issues	 34
Documentation Updates	 35
Migration, Upgrade, and Downgrade Instructions	 36
Product Compatibility	 37

Known Behavior

IN THIS SECTION

- [Authentication, Authorization, and Accounting \(AAA\) \(RADIUS\)](#) | 32
- [High Availability \(HA\) and Resiliency](#) | 32

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 17.3R1 for the EX Series.

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

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

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

High Availability (HA) and Resiliency

- During a nonstop software upgrade (NSSU) on an EX4300 Virtual Chassis, a traffic loop or loss might occur if the Junos OS software version that you are upgrading and the Junos OS software version that you are upgrading use different internal message formats. [PR1123764](#)
- On an EX4300 or a QFX5100 Virtual Chassis, when you perform an NSSU, there might be more than five seconds of traffic loss for multicast traffic. [PR1125155](#)

SEE ALSO

New and Changed Features	 23
Changes in Behavior and Syntax	 30
Known Issues	 33
Resolved Issues	 34
Documentation Updates	 35
Migration, Upgrade, and Downgrade Instructions	 36
Product Compatibility	 37

Known Issues

IN THIS SECTION

- Platform and Infrastructure | 33
- Port Security | 33
- User Interface and Configuration | 33

This section lists the known issues in hardware and software in Junos OS Release 17.3R1 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.

Platform and Infrastructure

- On EX4300, EX4600, and QFX5100 switches, if a remote analyzer has an output IP address that is reachable through a route learned by BGP, the analyzer might be in a down state. [PR1007963](#)

Port Security

- 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](#)

User Interface and Configuration

- The **source-address-filter** statement is by default allowed to configure and commit on EX4300 switches but that is not the expected behavior. [PR1281290](#)

SEE ALSO

New and Changed Features 23
Changes in Behavior and Syntax 30
Known Behavior 31
Resolved Issues 34

[Documentation Updates | 35](#)

[Migration, Upgrade, and Downgrade Instructions | 36](#)

[Product Compatibility | 37](#)

Resolved Issues

IN THIS SECTION

- [Authentication, Authorization, and Accounting \(AAA\) \(RADIUS\) | 35](#)
- [Infrastructure | 35](#)
- [Layer 2 Features | 35](#)
- [Platform and Infrastructure | 35](#)

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.

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

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

Infrastructure

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

Layer 2 Features

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

Platform and Infrastructure

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

SEE ALSO

New and Changed Features 23
Changes in Behavior and Syntax 30
Known Behavior 31
Known Issues 33
Documentation Updates 35
Migration, Upgrade, and Downgrade Instructions 36
Product Compatibility 37

Documentation Updates

IN THIS SECTION

- [Traffic Management User Guide for EX4600 Switches | 36](#)

This section lists the errata and changes in Junos OS Release 17.3R1 for the EX Series switches documentation.

Traffic Management User Guide for EX4600 Switches

- **Consolidation of the Traffic Management User Guide for QFX Series and EX4600 Switches (EX4600)**—Starting in Junos OS Release 17.3R1, the following three traffic management guides are consolidated into one user guide:
 - Traffic Management User Guide for QFX Series
 - Traffic Management User Guide for QFX 10000 Series
 - Traffic Management User Guide for EX4600 Switches

[See [Traffic Management User Guide for QFX Series and EX4600 Switches](#).]

SEE ALSO

[New and Changed Features | 23](#)

[Changes in Behavior and Syntax | 30](#)

[Known Behavior | 31](#)

[Known Issues | 33](#)

[Resolved Issues | 34](#)

[Migration, Upgrade, and Downgrade Instructions | 36](#)

[Product Compatibility | 37](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 37](#)

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

SEE ALSO

New and Changed Features 23
Changes in Behavior and Syntax 30
Known Behavior 31
Known Issues 33
Resolved Issues 34
Documentation Updates 35
Product Compatibility 37

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 38](#)

Hardware Compatibility

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

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

Hardware Compatibility Tool

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

SEE ALSO

New and Changed Features	 23
Changes in Behavior and Syntax	 30
Known Behavior	 31
Known Issues	 33
Resolved Issues	 34
Documentation Updates	 35
Migration, Upgrade, and Downgrade Instructions	 36

Junos OS Release Notes for Junos Fusion Data Center

IN THIS SECTION

- [New and Changed Features](#) | 39
- [Changes in Behavior and Syntax](#) | 39
- [Known Behavior](#) | 40
- [Known Issues](#) | 41
- [Resolved Issues](#) | 41
- [Documentation Updates](#) | 42

- Migration, Upgrade, and Downgrade Instructions | 42
- Product Compatibility | 56

These release notes accompany Junos OS Release 17.3R1 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

There are no new features in Junos OS Release 17.3R1 for Junos Fusion Data Center.

SEE ALSO

Changes in Behavior and Syntax 39
Known Behavior 40
Known Issues 41
Resolved Issues 41
Documentation Updates 42
Migration, Upgrade, and Downgrade Instructions 42
Product Compatibility 56

Changes in Behavior and Syntax

There are no changes in behavior and syntax for Junos Fusion Data Center in Junos OS Release 17.3R1.

SEE ALSO

New and Changed Features 39
Known Behavior 40

Known Issues	 41
Resolved Issues	 41
Documentation Updates	 42
Migration, Upgrade, and Downgrade Instructions	 42
Product Compatibility	 56

Known Behavior

IN THIS SECTION

- [Junos Fusion Data Center](#) | 40

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 17.3R1 for Junos Fusion Data Center.

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

Junos Fusion Data Center

- When a QFX10002 switch functions as an aggregation device in a Junos Fusion Data Center topology, it only supports cascade port-based slot assignments for satellite devices. In addition, any change in the configuration for a cascade port connected to a satellite device is treated as a catastrophic event and results in the deletion of any related interface state (including the extended ports), which is rebuilt after a period of time. The following additional restrictions also apply:
 - You cannot configure dual-homed satellite device extended ports as pure Layer 3 interfaces. As a result, **family inet** and **family inet6** are not supported on dual-homed extended ports.
 - If the ICL interface goes down, traffic loss will occur. As a workaround, we recommend you configure the ICL interface over an aggregated Ethernet interface with multiple links in the bundle to prevent single-point failures that would cause the ICL interface to shut down.

SEE ALSO

New and Changed Features	 39
--	----------------------

Changes in Behavior and Syntax	 39
Known Issues	 41
Resolved Issues	 41
Documentation Updates	 42
Migration, Upgrade, and Downgrade Instructions	 42
Product Compatibility	 56

Known Issues

There are no known issues in hardware and software in Junos OS Release 17.3R1 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	 39
Changes in Behavior and Syntax	 39
Known Behavior	 40
Resolved Issues	 41
Documentation Updates	 42
Migration, Upgrade, and Downgrade Instructions	 42
Product Compatibility	 56

Resolved Issues

There are no fixed issues in Junos OS 17.3R1 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.

SEE ALSO

New and Changed Features	 39
Changes in Behavior and Syntax	 39
Known Behavior	 40
Known Issues	 41
Documentation Updates	 42
Migration, Upgrade, and Downgrade Instructions	 42
Product Compatibility	 56

Documentation Updates

This section lists the errata or changes in Junos OS Release 17.3R1 for Junos Fusion Data Center documentation.

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

SEE ALSO

New and Changed Features	 39
Changes in Behavior and Syntax	 39
Known Behavior	 40
Known Issues	 41
Resolved Issues	 41
Migration, Upgrade, and Downgrade Instructions	 42
Product Compatibility	 56

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading an Aggregation Device](#) | 43
- [Preparing the Switch for Satellite Device Conversion](#) | 45
- [Autoconverting a Switch into a Satellite Device](#) | 47
- [Manually Converting a Switch into a Satellite Device](#) | 50

- [Configuring a Switch into a Satellite Device Before Connecting It to a Junos Fusion Topology | 52](#)
- [Configuring Satellite Device Upgrade Groups | 53](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 55](#)
- [Downgrading from Release 17.3R1 | 55](#)

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for Junos Fusion Data Center. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

Basic Procedure for Upgrading an Aggregation Device

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

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

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

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

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

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

```
user@host> request system software add reboot
source/jinstall-host-qfx-10-f-17.3R1.n-domestic-signed.tgz
```

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

```
user@host> request system software add reboot
source/jinstall-host-qfx-10-f-17.3R1.n-domestic-signed.tgz
```

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

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

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

- **ftp://hostname/pathname**
- **http://hostname/pathname**
- **scp://hostname/pathname** (available only for Canada and U.S. version)

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

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

Rebooting occurs only if the upgrade is successful.

Preparing the Switch for Satellite Device Conversion

Satellite devices in a Junos Fusion topology use a satellite software package that is different from the standard Junos OS software package. Before you can install the satellite software package on a satellite device, you first need to upgrade the target satellite device to an interim Junos OS software version that can be converted to satellite software. [Table 1 on page 45](#) shows a support matrix that maps Junos OS software used in aggregation devices to the compatible preconverted switch software and satellite device software.

Table 1: Aggregation Device Junos OS Software Compatibility with Satellite Software

Aggregation Device Version	Switch Version (preconversion)	Satellite Device Software Version
Junos OS Release 17.3R1	Junos OS Release 14.1X53-D43 or later	3.1R1

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**.

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.

Autoconverting a Switch into a Satellite Device

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

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

Before you begin:

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

To autoconvert a switch into a satellite device:

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

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

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

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

2. Log in to the aggregation device.
3. Configure the cascade ports.

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

[edit]

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

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

Examples:

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

```
[edit]
```

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

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

```
[edit]
```

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

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

```
[edit]
```

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

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

```
[edit]
```

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

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

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

```
[edit]
```

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

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

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

```
[edit]
```

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

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

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

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

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

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

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

7. Enable automatic satellite conversion:

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

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

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

8. Commit the configuration:

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

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

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

Manually Converting a Switch into a Satellite Device

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

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

Before you begin:

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

To manually convert a switch into a satellite device:

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

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

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

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

Examples:

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

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

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

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

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

```
[edit]
```

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

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

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

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

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

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

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

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

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

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

6. Manually configure the switch into a satellite device:

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

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

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

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

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

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

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

Before you begin:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Commit the configuration.

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

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

Configuring Satellite Device Upgrade Groups

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

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

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

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

```
[edit]
```

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

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

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

```
[edit]
```

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

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

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

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

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

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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


You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

Downgrading from Release 17.3R1

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

 **NOTE:** You cannot downgrade more than three releases.

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

SEE ALSO

New and Changed Features 39
Changes in Behavior and Syntax 39
Known Behavior 40
Known Issues 41
Resolved Issues 41
Documentation Updates 42
Product Compatibility 56

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 56

Hardware Compatibility

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

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

SEE ALSO

New and Changed Features 39
Changes in Behavior and Syntax 39
Known Behavior 40
Known Issues 41
Resolved Issues 41
Documentation Updates 42
Migration, Upgrade, and Downgrade Instructions 42

Junos OS Release Notes for Junos Fusion Enterprise

IN THIS SECTION

- New and Changed Features | 57
- Changes in Behavior and Syntax | 59
- Known Behavior | 59
- Known Issues | 60
- Resolved Issues | 61
- Documentation Updates | 62
- Migration, Upgrade, and Downgrade Instructions | 63
- Product Compatibility | 71

These release notes accompany Junos OS Release 17.3R1 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 | 58

This section describes the new features and enhancements to existing features in Junos OS Release 17.3R1 for Junos Fusion Enterprise.

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

Junos Fusion Enterprise

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

SEE ALSO

Changes in Behavior and Syntax	59
Known Behavior	59
Known Issues	60
Resolved Issues	61
Documentation Updates	62
Migration, Upgrade, and Downgrade Instructions	63
Product Compatibility	71

Changes in Behavior and Syntax

IN THIS SECTION

- [Junos Fusion Enterprise | 59](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 17.3R1 for Junos Fusion Enterprise.

Junos Fusion Enterprise

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

SEE ALSO

New and Changed Features 57
Known Behavior 59
Known Issues 60
Resolved Issues 61
Documentation Updates 62
Migration, Upgrade, and Downgrade Instructions 63
Product Compatibility 71

Known Behavior

IN THIS SECTION

- [Junos Fusion Enterprise | 60](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 17.3R1 for Junos Fusion Enterprise.

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

Junos Fusion Enterprise

- In a Junos Fusion Enterprise topology with dual aggregation devices, firewall statistics are not synced across the aggregation devices. [PR1105612](#)
- In a Junos Fusion Enterprise, in order to use a non-default port as a clustering port in a clustering port policy, the policy must include at least one port that is a default uplink/clustering port for that platform. [PR1241808](#)

SEE ALSO

New and Changed Features 57
Changes in Behavior and Syntax 59
Known Issues 60
Resolved Issues 61
Documentation Updates 62
Migration, Upgrade, and Downgrade Instructions 63
Product Compatibility 71

Known Issues

IN THIS SECTION

- [Junos Fusion Enterprise | 61](#)

This section lists the known issues in hardware and software in Junos OS Release 17.3R1 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 Enterprise with dual aggregation devices (ADs), if you apply Routing Engine loopback filters and bring down the cascade port on one of the ADs, the satellite device (SD) on the AD where the cascade port is down goes to ProvSessDown due to a TCP session drop over the ICL interface. As a workaround, add additional filters to bypass the ICL traffic for the ICL interface's IP address. [PR1275290](#)
- While applying a loopback filter on aggregation devices in a Junos Fusion Enterprise, Callback Control Protocol (CBCP) packets might be filtered, which might cause CBCP sessions to be dropped and one of the satellite devices in a redundant pair to be in the SplitBrainDn state. To work around this issue, you can add a filter similar to the following to the existing set of loopback filters:

```
set firewall family inet filter accept-icl term accept-icl from source-address 10.0.0.0/30
set firewall family inet filter accept-icl term accept-icl from destination-address 10.0.0.0/30
```

[PR1183680](#)

SEE ALSO

New and Changed Features 57
Changes in Behavior and Syntax 59
Known Behavior 59
Resolved Issues 61
Documentation Updates 62
Migration, Upgrade, and Downgrade Instructions 63
Product Compatibility 71

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 17.3R1 | 62](#)

This section lists the issues fixed in Junos OS Release 17.3R1.

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

Resolved Issues: 17.3R1

Junos Fusion Enterprise

- On a Junos Fusion Enterprise, an upgrade group's association with a satellite software version is removed if the chassis satellite-management redundancy-groups configuration is deleted. [PR1267370](#)
- On Junos Fusion Enterprise, traffic shaping is not supported on the extended ports. [PR1268084](#)
- When a race condition results in a dynamic VLAN assignment, the MAC-based VLAN (MBV) entry might not get created on the peer AD. This situation can result in traffic loss when it flows through the peer AD. [PR1282828](#)
- VRRP has a split brain in dual autodiscovery Junos Fusion. [PR1293030](#)

SEE ALSO

New and Changed Features 57
Changes in Behavior and Syntax 59
Known Behavior 59
Known Issues 60
Documentation Updates 62
Migration, Upgrade, and Downgrade Instructions 63
Product Compatibility 71

Documentation Updates

There are no errata or changes in Junos OS Release 17.3R1 for Junos Fusion Enterprise documentation.

SEE ALSO

New and Changed Features 57
Changes in Behavior and Syntax 59
Known Behavior 59

[Known Issues | 60](#)

[Resolved Issues | 61](#)

[Migration, Upgrade, and Downgrade Instructions | 63](#)

[Product Compatibility | 71](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading Junos OS on an Aggregation Device | 63](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 66](#)
- [Preparing the Switch for Satellite Device Conversion | 66](#)
- [Converting a Satellite Device to a Standalone Switch | 67](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 69](#)
- [Downgrading from Release 17.3 | 70](#)

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

Basic Procedure for Upgrading Junos OS on an Aggregation Device

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

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

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

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

To download and install Junos OS Release 17.3R1:

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

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

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

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

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

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

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

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

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

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

Rebooting occurs only if the upgrade is successful.

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

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

Preparing the Switch for Satellite Device Conversion

There are multiple methods to upgrade or downgrade satellite software in your Junos Fusion Enterprise. See [Configuring or Expanding a Junos Fusion Enterprise](#).

For satellite device hardware and software requirements, see [Understanding Junos Fusion Enterprise Software and Hardware Requirements](#).

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

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

NOTE: 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. (EX3400 and EX4300 switches only) After the reboot is complete, convert the built-in 40-Gbps QSFP+ interfaces from Virtual Chassis ports (VCPs) into network ports:

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

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

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

This step is required for the 40-Gbps QSFP+ interfaces that will be used as uplink interfaces in a Junos Fusion topology. Built-in 40-Gbps QSFP+ interfaces on EX3400 and EX4300 switches are configured into VCPs by default, and the default settings are restored after the device is reset.

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

Converting a Satellite Device to a Standalone Switch

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

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

1. Using a Web browser, navigate to the Junos OS software download URL on the Juniper Networks webpage:
<https://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** from the menu and select the switch platform series and model for your satellite device.
4. Select the software image for your platform. For satellite device software requirements, see [Understanding Junos Fusion Enterprise Software and Hardware Requirements](#).
5. Review and accept the End User License Agreement.
6. Download the software to a local host.
 Copy the software to the routing platform or to your internal software distribution site.

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

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

[edit]

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

For example, to remove member number 101 from the Junos Fusion:

[edit]

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

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

8. Commit the configuration.

To commit the configuration to both Routing Engines:

[edit]

```
user@aggregation-device# commit synchronize
```

To commit the configuration to a single Routing Engine:

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

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

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

For example, to install a software package stored in the `/var/tmp` directory on the aggregation device onto an EX4300 switch acting as the satellite device using FPC slot 102:

```
[edit]
user@aggregation-device> request chassis satellite install
/var/tmp/jinstall-ex-4300-14.1X53-D43.n-domestic-signed.tgz fpc-slot 102
```

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

Downgrading from Release 17.3

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

NOTE: You cannot downgrade more than three releases.

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

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

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

SEE ALSO

[New and Changed Features | 57](#)

[Changes in Behavior and Syntax | 59](#)

[Known Behavior | 59](#)

[Known Issues | 60](#)

[Resolved Issues | 61](#)

[Documentation Updates | 62](#)

[Product Compatibility | 71](#)

Product Compatibility

IN THIS SECTION

- [Hardware and Software Compatibility | 71](#)
- [Hardware Compatibility Tool | 71](#)

Hardware and Software Compatibility

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

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

Hardware Compatibility Tool

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

SEE ALSO

New and Changed Features 57
Changes in Behavior and Syntax 59
Known Behavior 59
Known Issues 60
Resolved Issues 61
Documentation Updates 62
Migration, Upgrade, and Downgrade Instructions 63

Junos OS Release Notes for Junos Fusion Provider Edge

IN THIS SECTION

- New and Changed Features | 72
- Changes in Behavior and Syntax | 74
- Known Behavior | 74
- Known Issues | 75
- Resolved Issues | 75
- Documentation Updates | 76
- Migration, Upgrade, and Downgrade Instructions | 76
- Product Compatibility | 84

These release notes accompany Junos OS Release 17.3R1 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

- Junos Fusion | 73

This section describes the new features and enhancements to existing features in Junos OS Release 17.3R1 for Junos Fusion Provider Edge.

Junos Fusion

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

In a Junos Fusion system, PoE is used to carry electric power from an extended port on a satellite device to a connected device. An extended port is any network-facing port on a satellite device in a Junos Fusion Provider Edge. All extended ports that support PoE on satellite devices in a Junos Fusion Provider Edge support the IEEE 802.3at PoE+ standard. The aggregation device on Junos Fusion Provider Edge manages PoE support of PoE-capable interfaces on satellite device. Junos Fusion Provider Edge only supports PoE with EX series switches as satellite devices and a MX Series 3D Universal Router as the aggregation device.

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

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

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

- **Metro Ethernet Forum (MEF)Carrier Ethernet 2.0 Certification**—Starting in Junos OS Release 17.3R1, Junos Fusion Provider Edge qualifies for Carrier Ethernet 2.0 (CE2.0) certification. This ensures that the routers and switches in a Junos Fusion Provider Edge system comply withto the Carrier Ethernet specification set by the MEF.

SEE ALSO

Changes in Behavior and Syntax 74
Known Behavior 74
Known Issues 75
Resolved Issues 75
Documentation Updates 76
Migration, Upgrade, and Downgrade Instructions 76
Product Compatibility 84

Changes in Behavior and Syntax

There are no changes in default behavior and syntax for Junos Fusion Provider Edge in Junos OS Release 17.3R1.

SEE ALSO

[New and Changed Features | 72](#)

[Known Behavior | 74](#)

[Known Issues | 75](#)

[Resolved Issues | 75](#)

[Documentation Updates | 76](#)

[Migration, Upgrade, and Downgrade Instructions | 76](#)

[Product Compatibility | 84](#)

Known Behavior

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 17.3R1 for Junos Fusion Provider Edge.

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

SEE ALSO

[New and Changed Features | 72](#)

[Changes in Behavior and Syntax | 74](#)

[Known Issues | 75](#)

[Resolved Issues | 75](#)

[Documentation Updates | 76](#)

[Migration, Upgrade, and Downgrade Instructions | 76](#)

[Product Compatibility | 84](#)

Known Issues

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

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

SEE ALSO

New and Changed Features	 72
Changes in Behavior and Syntax	 74
Known Behavior	 74
Resolved Issues	 75
Documentation Updates	 76
Migration, Upgrade, and Downgrade Instructions	 76
Product Compatibility	 84

Resolved Issues

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

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

SEE ALSO

New and Changed Features	 72
Changes in Behavior and Syntax	 74
Known Behavior	 74
Known Issues	 75
Documentation Updates	 76
Migration, Upgrade, and Downgrade Instructions	 76
Product Compatibility	 84

Documentation Updates

There are no errata or changes in Junos OS Release 17.3R1 for Junos Fusion Provider Edge documentation.

SEE ALSO

- [New and Changed Features | 72](#)
- [Changes in Behavior and Syntax | 74](#)
- [Known Behavior | 74](#)
- [Known Issues | 75](#)
- [Resolved Issues | 75](#)
- [Migration, Upgrade, and Downgrade Instructions | 76](#)
- [Product Compatibility | 84](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading an Aggregation Device | 77](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 79](#)
- [Preparing the Switch for Satellite Device Conversion | 79](#)
- [Converting a Satellite Device to a Standalone Device | 81](#)
- [Upgrading an Aggregation Device | 83](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 83](#)
- [Downgrading from Release 17.3 | 83](#)

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

Basic Procedure for Upgrading an Aggregation Device

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

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

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

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

The download and installation process for Junos OS Release 17.3R1 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 17.3R1 **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](#)

Customers with EX4300 switches, use the following command:

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

Customers with QFX5100 switches, use the following command:

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

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

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

2. Clear the device:

```
[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 the satellite device from the Junos Fusion topology.

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

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

1. Using a Web browser, navigate to the Junos OS software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads>
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology > Junos Platform > Junos Fusion** from the drop-down list and select the switch platform series and model for your satellite device.
4. Select the Junos OS Release 14.1X53-D43 software image for your platform.
5. Review and accept the End User License Agreement.
6. Download the software to a local host.
7. Copy the software to the routing platform or to your internal software distribution site.
8. Remove the satellite device from the automatic satellite conversion configuration.

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

[edit]

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

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

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

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

9. Commit the configuration.

To commit the configuration to both Routing Engines:

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

Otherwise, commit the configuration to a single Routing Engine:

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

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

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

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

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

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

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

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

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

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

Upgrading an Aggregation Device

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

Downgrading from Release 17.3

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

NOTE: You cannot downgrade more than three releases.

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

SEE ALSO

New and Changed Features 72
Changes in Behavior and Syntax 74
Known Behavior 74
Known Issues 75
Resolved Issues 75
Documentation Updates 76
Product Compatibility 84

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 84](#)

Hardware Compatibility

Hardware Compatibility

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

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

Hardware Compatibility Tool

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

SEE ALSO

New and Changed Features 72
Changes in Behavior and Syntax 74
Known Behavior 74
Known Issues 75
Resolved Issues 75
Documentation Updates 76
Migration, Upgrade, and Downgrade Instructions 76

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

IN THIS SECTION

- [New and Changed Features | 86](#)
- [Changes in Behavior and Syntax | 110](#)
- [Known Behavior | 115](#)
- [Known Issues | 116](#)
- [Resolved Issues | 123](#)
- [Documentation Updates | 128](#)
- [Migration, Upgrade, and Downgrade Instructions | 129](#)
- [Product Compatibility | 136](#)

These release notes accompany Junos OS Release 17.3R1 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- Class of Service (CoS) | 87
- Dynamic Host Configuration Protocol (DHCP) | 87
- EVPNs | 88
- General Routing | 90
- High Availability (HA) and Resiliency | 90
- Interfaces and Chassis | 91
- IPSec | 93
- IPv6 | 93
- Layer 2 Features | 93
- Layer 2 VPN | 94
- Layer 3 Features | 95
- Management | 95
- MPLS | 96
- Multicast | 97
- Network Management and Monitoring | 98
- Operation, Administration, and Maintenance (OAM) | 98
- Port Security | 100
- Routing Policy and Firewall Filters | 100
- Routing Protocols | 101
- Security | 103
- Services Applications | 103
- Software Defined Networking (SDN) | 105
- Subscriber Management and Services | 105
- Virtual Chassis | 110

This section describes the new features and enhancements to existing features in Junos OS Release 17.3R1 for the MX Series routers.

Class of Service (CoS)

- **Support for efficient use of CoS resources on targeted interfaces (MX Series)**—Starting in Junos OS Release 17.3R1, when you configure Junos OS to target the egress traffic for a subscriber on a single member link, Junos OS applies CoS resources only to the active link, optimizing the use of available scheduling nodes. If the assigned primary link goes down, CoS scheduling resources are switched to the backup link.

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

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

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

Dynamic Host Configuration Protocol (DHCP)

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

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

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

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

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

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

For a DHCP dual-stack subscriber, the DHCPv4 and DHCPv6 protocol handshakes are generally completely independent of each other. So it is theoretically possible that each arm of a given dual-stack

subscriber could connect to a different BNG. A configured mode of operation is supported to avoid this scenario

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

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

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

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

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

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

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

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

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

EVPNs

- **EVPN-VXLAN support for VXLAN Gateways using an IPv6 underlay (MX Series with MPC and MIC)**—Starting in Junos OS Release 17.3R1, MX Series routers with MPC and MIC interfaces extend support for Virtual Extensible LAN (VXLAN) gateways from IPv4 to IPv6 underlays. With this feature

enhancement, each VXLAN gateway supports the following functionalities in addition to the IPv4 functionalities already supported:

- VLAN-based service
- VLAN-bundle service
- Port-based service
- VLAN-aware service

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

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

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

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

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

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

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

General Routing

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

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

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

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

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

High Availability (HA) and Resiliency

- **Mandatory action before initiating GRES in the presence of PIC bounce alarms (MX10003 router)**—In Junos OS Release 17.3R1, before initiating graceful Routing Engine switchover (GRES) on an MX10003, you must clear all the PIC bounce alarms. Otherwise, it will provide negative results as the alarms are not preserved on GRES currently. It may also result in unstable behavior of MPC.

Consider the example of PIC bounce alarm shown here. In this case, you must clear the PIC need bounce alarm before the switchover.

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

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

[See [Understanding VRRP](#)]

Interfaces and Chassis

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

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

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

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

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

- **MPCs, PICs, and MICs supported on MX10003 routers**—Starting with Junos OS Release 17.3R1, MX10003 router MPC contains 3 EA ASICs that operates in 400G mode. MX10003 router contains EA (Eagle ASIC) based line card. Each MPC supports a built-in PIC and a modular MICs, JNP-MIC1 (MIC without MACsec support) and JNP-MIC1-MACSEC (MIC with MACsec support). The fixed port PIC is mapped to PIC-0 and each PFE is mapped to 2 ports in PIC-0. The MIC is mapped to PIC-1 and each PFE will be mapped to 4 ports in PIC-1. The PIC/MIC ports on MX10003 router MPCs support multiple port speeds (10/40/100GE). Hence, these ports are classified as multi rate ports. However, all the PIC/MIC ports do not support all the port speeds. On MPC all the 12 ports are active and are capable of running in 100G, 40G and 4x10G mode.
- **Support for inline flow monitoring on MPCs on MX10003 routers**—Starting with Junos OS Release 17.3R1, MPCs on MX10003 router support inline flow monitoring. Inline flow monitoring results in higher scalability and performance, as the scaling and performance are not dependent on the capacity

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

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

The new sensors are grouped into the following functional areas:

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

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

IPSec

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

IPv6

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

Layer 2 Features

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

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

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

Layer 2 VPN

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

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

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

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

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

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

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

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

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

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

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

Layer 3 Features

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

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

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

Management

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

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

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

Additionally, the following paths are also now supported:

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

`bgp/neighbors/neighbor/afi-safis/afi-safi/state/queues/output`

- `/network-instances/network-instance/protocols/protocol/
bgp/neighbors/neighbor/afi-safis/afi-safi/state/queues/input`
- `/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/state/ImportEval`
- `/network-instances/network-instance/protocols/protocol/
bgp/neighbors/neighbor/state/ImportEvalPending`

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

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

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

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

- **Junos Telemetry Interface support (MX10003 and MX204)**—Starting with Junos OS Release 17.3R1, MX10003 and MX204 routers support the Junos Telemetry Interface, which enables you to provision sensors to export telemetry data for various network elements. To provision sensors to stream data through UDP, all parameters are configured at the **[edit services analytics]** hierarchy level. To provision sensors to stream data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters for a specified list of OpenConfig command paths. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models.

MPLS

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

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

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

- **Support for features on MPC7E, MPC8E, and MPC9E line cards (MX Series)**—In Junos OS Release 17.3R1, MPC7E, MPC8E, and MPC9E support the following features:
 - LDP uses the longest match to learn the routes aggregated or summarized across OSPF areas or IS-IS levels in the interdomain.
 - Support for notifications on the service node when the access pseudowire goes down, and efficient termination capabilities when Layer 2 and Layer 3 segments are interconnected.
[See [Pseudowire Termination: Explicit Notifications for Pseudowire Down](#).]
 - BGP PIC Edge for RSVP enables you to implement a solution where a protection path is calculated in advance to provide an alternative forwarding path in case of path failure.
[See [show rsvp version](#).]
 - Circuit cross-connect (CCC) encapsulation is supported on the transport side of an MPLS pseudowire subscriber logical interface. This feature helps in migrating or deploying seamless MPLS architectures in access networks.
[See [Pseudowire Subscriber Logical Interfaces Overview](#).]
 - inet and inet6 families are supported on the services side of an MPLS pseudowire subscriber as well as non subscriber logical interfaces.
 - Distributed denial-of-service (DDoS) protection is supported on the services side of an MPLS pseudowire subscriber logical interface.
 - Policer and filter are supported on the services side of an MPLS pseudowire subscriber logical interface.
 - Accurate transmit logical interface statistics are supported on the services side of an MPLS pseudowire subscriber logical interface.
 - Inline IPFIX is supported on the services side of an MPLS pseudowire subscriber logical interface.
 - Port mirroring is supported on the services side of an MPLS pseudowire subscriber logical interface.

Multicast

- **PIM resolve type-length-value (TLV) for multicast in seamless MPLS (MX Series)**—Starting in Junos OS Release 17.3R1, Junos OS adds support for RFC 5496, Reverse Path Forwarding (RPF) Vector TLV . With this support, Protocol Independent Multicast (PIM) can be used in environments where the core routers do not maintain external routes, for example in a seamlessMPLS network.
[See [rpf-vector](#).]
- **Support for IPv6 multicast Rosen version 7 (MX Series)**—Starting in Junos OS Release 17.3R1, Junos OS multicast support extends to the default multicast distribution tree (MDT) for Rosen 7 multicast virtual private networks (MVPN) and data MDT for both Rosen 6 (PIM-ASM) and Rosen 7 (PIM-SSM). The IPv6 support applies to the customer space only.
[See [Draft-Rosen Multicast VPNs Overview](#) .]

Network Management and Monitoring

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

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

Operation, Administration, and Maintenance (OAM)

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

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

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

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

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

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

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

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

Port Security

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

Routing Policy and Firewall Filters

- **Support for packet forwarding features (MX150)**—Starting in Junos OS Release 17.3R1, the MX150 supports the following key packet forwarding features:
 - Basic Layer 2 features and protocols—You can configure layer 2 features that can vary from the very simple (aggregated Ethernet trunk interfaces, spanning trees), to the more complex (inner and outer VLAN tags, broadcast domains), to the very complicated (integrated bridging and routing, layer 2 filtering).
 - Class of service (CoS)—You can configure CoS features to provide multiple classes of service for different applications. CoS enables you to divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs. It enables you to provide differentiated services when best-effort traffic delivery is insufficient.
 - Firewall filters and policers—You can configure firewall filters that define whether to accept or discard packets. You can use firewall filters on interfaces, VLANs, routed VLAN interfaces (RVIs), link aggregation groups (LAGs), and loopback interfaces. You can use policing to apply limits to traffic flow and specify the action to be taken for packets that exceed those limits.
 - Port mirroring—Port mirroring copies packets entering or exiting a port or entering a VLAN and sends the copies to a local interface for local monitoring. You can use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on.
- **Bypass loopback with firewall filter tunnel encapsulation (MX Series)**—Starting in Junos OS Release 17.3R1, static filter based generic routing encapsulation (GRE) tunnels no longer use a loopback stream for transit traffic. The new default, which allows for increased bandwidth utilization on MPCs using the MX Series chipset, is to skip the loopback. In addition, support for IPv4 as the outer IP is available (the inner payload supports both IPv4 and IPv6). Egress sampling on the outer header is not affected. This change does not apply to GRE in UDP or to dynamic tunnels.

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

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

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

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

set firewall tunnel-end-point *tunnel* gre

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

Routing Protocols

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Security

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

Services Applications

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

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

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

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

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

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

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

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

the `[edit chassis fpc slot-number inline-services flow-table-size]` hierarchy level. The existing limit on `flow-export-rate` under `inline-jflow` for each family in the sampling instance is increased to 3200 from 400.

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

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

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

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

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

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

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

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

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

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

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

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

Software Defined Networking (SDN)

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

[See [Junos Node Slicing](#)]

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

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

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

Subscriber Management and Services

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

- tunnel-medium-type—RADIUS attribute 65, Tunnel-Medium-Type
- tunnel-server-auth-id—RADIUS attribute 91, Tunnel-Server-Auth-Id
- tunnel-server-endpoint—RADIUS attribute 67, Tunnel-Server-Endpoint
- tunnel-type—RADIUS attribute 64, Tunnel-Type

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

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

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

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

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

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

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

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

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

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

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

- **Support for sending LAC NAS-port and LAC IP-address attributes to RADIUS for MX Routers**—Starting in Junos OS Release 17.3R1, you can override the following at the **[edit access profile set radius options override]** hierarchy level:
 - **nas-port** with the LAC side **nas-port** information.
 - **nas-ip-address** with the I2tp LAC endpoint IP address information.
- **Support for load-based throttling of subscribers (MX Series)**—Starting in Junos OS Release 17.3R1, the **no-load-throttling** statement disables line card load-based throttling when configured at the **[edit system services resource-monitor]** hierarchy level. Load-based throttling is also disabled when the **no-throttle** statement is configured at the **[edit system services resource-monitor]** hierarchy level.
- **DDoS protection flow detection for enhanced subscriber management (MX Series Routers)**—Starting in Junos OS Release 17.3R1, enhanced subscriber management supports flow detection for DDoS protection. Enable flow detection by including the **flow-detection** statement at the **[edit system ddos-protection global]** hierarchy level. Flows that violate a DDoS protection policer are tracked as suspicious flows; they become culprit flows when they violate the policer bandwidth for the duration of a configurable detection period. Culprit flows are dropped, kept, or policed to below the allowed bandwidth level. Suspicious flow tracking stops if the violation stops before the detection period expires.

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

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

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

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

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

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

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

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

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

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

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

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

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

- **Disabling RADIUS-initiated subscriber secure policy mirroring (MX Series)**—Starting in Junos OS Release 17.3R1, you can use the `dtcp-only` statement to prevent RADIUS-initiated subscriber secure policy mirroring from being enabled, while allowing both DTCP-initiated mirroring and DTCP-based flow-tap services (FlowTapLite) to be enabled. Requests from RADIUS to attach a subscriber secure policy (mirroring service) to a subscriber are rejected. This statement has no effect on existing RADIUS-initiated

mirroring services. You must issue the statement before such services are activated for a subscriber. Subscriber login and session establishment are not affected.

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

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

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

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

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

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

Virtual Chassis

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

SEE ALSO

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

[Known Behavior | 115](#)

[Known Issues | 116](#)

[Resolved Issues | 123](#)

[Documentation Updates | 128](#)

[Migration, Upgrade, and Downgrade Instructions | 129](#)

[Product Compatibility | 136](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [EVPNs | 111](#)
- [General Routing | 111](#)
- [Interfaces and Chassis | 111](#)
- [Management | 111](#)
- [Network Management and Monitoring | 112](#)
- [Routing Protocols | 113](#)
- [Services Application | 113](#)
- [Subscriber Management and Services | 113](#)
- [VLAN Infrastructure | 114](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 17.3R1 for MX Series routers.

EVPNs

- **commit check command successful with trunk port and EVPN-MPLS/EVPN-VXLAN EVI configured**—As of Junos OS Release 17.3, when adding a trunk port with dual tags to an EVPN and MPLS routing instance, or an EVPN and VXLAN routing instance, the CLI commit check configuration considers the **inner-vlan-id-list** statement and is successful.

General Routing

- **Change in boot up behavior(MX10003)**—Starting in Junos OS Release 17.3R1, when the MPC is removed and plugged into the slot, the MPC is brought online automatically. In Junos OS 17.3R1 prior releases, the MPC could be brought online only after issuing the **request chassis fpc slot number online** command.
- **Commit Preparation on MX-VC setup**—On MX Series virtual chassis setup, you see the following:
 - When you issue **commit prepare** on one Routing Engine followed by switchover, the Routing Engine where the switchover command is issued reboots. Therefore, the prepared cache gets cleared in that Routing Engine.
 - **clear system commit prepared** clears the plus files and prepared cache only in the device where the command is issued.
- **Support for deletion of static routes when the BFD session goes down (MX Series)**—Starting with Junos OS Release 17.3R1, the default behavior of the static route at the [**edit routing-options static static-route bfd-admin-down**] hierarchy level is active. So, the static routes are deleted when the BFD receives a session down message.

Interfaces and Chassis

- **show chassis environment cb command not supported on MX10003 backup Routing Engine**—In Junos OS Release 17.3R1, you cannot get the environmental information about the Control Boards (CBs) installed in an MX10003 because the router does not support the **show chassis environment cb** CLI command on a backup Routing Engine. No output is displayed if you execute this command on an MX10003 backup Routing Engine.

Management

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

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

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

Network Management and Monitoring

- **Enhancement to SNMPv3 traps for contextName field (MX Series)**—Starting in Junos OS Release 17.2, the contextName field in SNMPv3 traps generated from a non-default routing instance, is populated with the same routing-instance information as is given in SNMPv2 traps. SNMPv2 traps provide the routing-instance information as context in the form of context@community. This information gives the network monitoring system (NMS) the origin of the trap, which is information it might need. But in SNMPv3, until now, the contextName field was empty. For traps originating from a default routing instance, this field is still empty, which now indicates that the origin of the trap is the default routing instance.
- **Enhancement to about-to-expire logic for license expiry syslog messages (MX Series)**—Starting in Junos OS Release 17.3R1, the logic for multiple capacity type licenses and when their expiry raises alarms was changed. Previously, the behavior had alarms and syslog messages for expiring licenses raised based on the highest validity, which would mislead users in the case of a license expiring earlier than the highest validity license. The new behavior has the about-to-expire logic based on the first expiring license.
- **SNMP syslog messages changed (MX Series)**—In Junos OS Release 17.3R1, two misleading SNMP syslog messages have been rewritten to accurately describe the event:
 - OLD—AgentX master agent failed to respond to ping. Attempting to re-register
NEW—AgentX master agent failed to respond to ping, triggering cleanup!
 - OLD—NET-SNMP version %s AgentX subagent connected
NEW—NET-SNMP version %s AgentX subagent Open-Sent!

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

Routing Protocols

- **Change in output of `show configuration routing-options flow operational` command**—Starting in Junos OS Release 17.3R1, the sequence of statements in the output of `show configuration routing-options flow` operational command has changed to improve readability. The **then** statements are now displayed after the **match** conditions in a logical sequence.
- **BGP GR stale routes are not removed when BFD goes down**—Starting in Junos OS Release 17.3R1, 17.2R2, 17.1R3, 16.2R3, 16.1R5, and 15.1R7, when a BGP session that has BFD configured without the **hold-down-interval** fails, the BFD session remains active. The BFD session is not impacted even when graceful restart is enabled. BGP deletes the BFD session when user explicitly disables BFD on a BGP peer. Note that BFD session is created only when a BGP session is **Established**. In earlier Junos OS releases, BFD sessions are deleted when the BGP session fails and the **hold-down-interval** option is not configured.

Services Application

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

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

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

Subscriber Management and Services

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

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

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

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

set system configuration-database max-db-size

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

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

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

VLAN Infrastructure

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

SEE ALSO

[New and Changed Features | 86](#)

[Known Behavior | 115](#)

[Known Issues | 116](#)

[Resolved Issues | 123](#)

[Documentation Updates | 128](#)

[Migration, Upgrade, and Downgrade Instructions | 129](#)

[Product Compatibility | 136](#)

Known Behavior

IN THIS SECTION

- [General Routing | 115](#)
- [High Availability \(HA\) and Resiliency | 115](#)

This section contains the known behavior, system maximums, and limitations in hardware and software in Junos OS Release 17.3R1 for MX Series routers.

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

General Routing

- On MX Series routers, parity memory errors occur in the pre classifier engines within an MPC. Packets silently discarded earlier are reported in syslogs and alarms when parity memory errors occur.
- On an MX10003 router, when the management interface (fxp0 or em0) is down on the master routing engine, in addition to the **Ethernet Link Down** alarm, an additional **Management Ethernet Link Down** alarm is also raised.

High Availability (HA) and Resiliency

- **MPC7E MPC8E and MPC9E line card restrictions for MX-VC ISSU (MX Series)**—MPC7E, MPC8E, and MPC9E line cards do not support ISSU in 17.3R1 for MX virtual chassis configurations, and these line cards must be removed or configured to power off during the MX-VC ISSU process. ISSU in 17.3R1 is supported for MX standalone chassis configurations.

[See [Preparing for a Unified ISSU in an MX Series Virtual Chassis](#)]

SEE ALSO

[New and Changed Features | 86](#)

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

[Known Issues | 116](#)

[Resolved Issues | 123](#)

[Documentation Updates | 128](#)

[Migration, Upgrade, and Downgrade Instructions | 129](#)

[Product Compatibility | 136](#)

Known Issues

IN THIS SECTION

- [Forwarding and Sampling | 116](#)
- [General Routing | 117](#)
- [Hardware | 120](#)
- [Infrastructure | 120](#)
- [Interfaces and Chassis | 121](#)
- [Layer 2 Features | 121](#)
- [MPLS | 121](#)
- [Platform and Infrastructure | 122](#)
- [Routing Protocols | 122](#)
- [Services Applications | 122](#)
- [VPN | 122](#)

This section lists the known issues in hardware and software in Junos OS Release 17.3R1 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.

Forwarding and Sampling

- The policing filter application to the LSP is catastrophic. Any active LSP that carries traffic after applying a policing filter tears down, resignals, and drops traffic for 2 seconds. [PR1160669](#)
- In some stress test conditions sampled crashed with core dump when connecting L2BSA and EVPN subscribers aggressively [PR1293237](#)

General Routing

- MX Series routers with FreeBSD 10.x might experience PCF and CHASSISD_I2CS_READBACK_ERROR. [PR1174001](#)
- 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. Netdev-interface resource assumes that speed is a configurable parameter which is supported on a GE interface but not on an XE interface. Hence netdev-interface resource cannot be used to configure an XE interface due to this limitation. This limitation is applicable to packages chef-11.10.4_1.1.*.tgz chef-11.10.4_2.0.*.tgz in all platforms {i386/x86-32/powerpc}. [PR1181475](#)
- On Junos OS platforms with MACsec enabled, adding or deleting MACsec or changing the interface configuration while MACsec is enabled might cause multiple security associations (SAs) to be active at the same time because of a key server timing contention, which results in the dot1x daemon (dot1xd) crash with a core file generated. The core files could be seen by executing the **show system core-dumps** CLI command. [PR1185928](#)
- Upgrading using unified ISSU might trigger a flap in the interfaces on MX Series routers. The following message might be seen: SFP: pointer Null, sfp_set_present. [PR1200045](#)
- In large-scale configurations or environments with high rates of churn, on MX Series routers with FPCs, ASIC memory might become fragmented over time. In an extreme case, it is possible that memory of a particular size might become exhausted. Also, because of the fragmentation, the available memory will not fulfill the pending allocation. [PR1216300](#)
- On MX Series routers with MPC2E-3D-NG, MPC2E-3D-NG-Q, MPC3E-3D-NG, and MPC3E-3D-NG-Q line cards, if the FPC-MIC link fails, the bridge might keep sending register messages in an infinite loop, which would cause continuous PCI exceptions. [PR1231167](#)
- When changing virtual switch type from IRB type to regular bridge, interfaces under openFlow protocol are all removed. The OpenFlow process (daemon) fails to program any flows. [PR1234141](#)
- With vLNS (vBNG), a commit generates a **warning: requires 'l2tp-inline-lns' license** but a valid license is installed. [PR1235697](#)
- On MX480, MX240, and MPC2-NG because of side cooling, the XM chip temperature might reach 67° C and fans only operate at normal speed. The XM chip has a total throughput performance of about 130 Gbps, but because of an increasing DDR memory refresh interval, the packet forwarding throughput will be reduced by about 3 to 4 percent out of the 130 Gbps range. If you reach this limit, fabric drop queuing counters will get reported. A syslog entry indicates the refresh interval is being increased. Junos OS software should be enhanced to set the fan to full speed before XM chip temperature reaches 67° C. [PR1244375](#)
- In MX10003 platform, CLI operational command **show chassis fpc errors** does not capture Packet Forwarding Engine state information, unlike other legacy MX Series platforms. [PR1249648](#)
- Duplicate sensor resources are created when the difference is a trailing "/". [PR1263446](#)

- Essentially, the issue is caused when an interface comes online and both OAM protocol and MKA protocol tries to establish their respective sessions. Because of contention between these two protocol OAM takes down the interface and MKA fails to establish connection (since interface is down it cant sent out MKA packets). [PR1265352](#)
- On an MX Series Virtual Chassis system in a scaled subscriber management scenario, when you perform an ISSU while protocol sessions are active, the protocols might go down and come back up again, which might cause traffic loss. [PR1265407](#)
- This is a very specific issue when Packet Forwarding Engine is oversubscribed with unknown unicast flood with no MAC learning, which is not a common configuration. During unified ISSU only the Packet Forwarding Engine is getting wedged. The issue is not seen when the Packet Forwarding Engine is oversubscribed with L3 traffic or with L2 traffic with MAC learning. [PR1265898](#)
- BBE advanced services are not supported on a Junos Node Slicing platform. Hence, mobility is disabled on a Junos Node Slicing platform BSYS and GNF Routing Engines. As a workaround, for legacy BBE functionality to work properly on Junos Node Slicing platform, reboot when the BSYS Routing Engine is changed to standalone Routing Engine mode (normal) and vice versa. [PR1266615](#)
- During a frequent STP state change over a link or a frequent link flap, some MAC addresses in the corresponding member link interface bridge domain might not be learned. [PR1268175](#)
- The command **show chassis led** on MX Series routers should not be displayed in possible completions of **show chassis** command, as this command is not valid for this platform. The issue is purely cosmetic. [PR1268848](#)
- The l2cpd process might generate a core file when lldp neighbors are cleared. [PR1270180](#)
- The mspmand incorrectly generates log messages about memory zone level This issue occurs every 49.7 days and recovers by itself. This is a display issue and will not affect traffic. [PR1273901](#)
- Device might not power up when crossover cable is used. It is advised to used straight cables. [PR1274613](#)
- Interfaces might flap on the 20x1GE SFP MIC when performing ISSU from Junos OS Release 17.3R1. [PR1276816](#)
- After a MS-MPC-PIC is offline, onlined, or bounced (due to AMS configuration change), sometimes PIC might approximately take 400 seconds to restart. [PR1280336](#)
- BIOS firmware upgrade or downgrade support not available with Junos OS 17.3R1 image. [PR1281050](#)
- If vmhost snapshot is taken on alternate disk and there is no further vmhost software image upgrade, the expectation is that on current vmhost image getting corrupted, system will boot with alternate disk so as user can recover primary disk to restore the state. However, under the condition where corruption is with host root file system, the node is booting with previous vmhost software as against booting from alternate disk. [1281554](#)
- While checking the diagnostic level of the optics using streaming telemetry, interfaces that are in a down state do not provide data. [PR1281943](#)

- On an MX Series Virtual Chassis, when using a channelized configuration on MPC7/8/9 MRATE PIC QSFP interfaces for VCP connections between members, a VCP interface needs to be configured on channel 0 of each QSFP to activate the port. [PR1283283](#)
- Unified ISSU not supported from Junos OS Release 15.1 onwards when source release includes one or more BBE features such as IFL options, CoS fragmentation map, MLPPP, advisory options, advanced services and multicast distribution.
- BBE ISSU will fail if source release has subscribers who use dynamic profile with any one of the below configuration. Recommendation for BBE ISSU is to deploy a Junos OS Release that has a fix for this PR for source as well as target release.

```

set dynamic-profiles <profile-name> class-of-service interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit" fragmentation-map <frag-map-name> set dynamic-profiles <profile-name>
interfaces pp0 unit "$junos-interface-unit" family mlppp bundle "$junos-bundle-interface-name" set
dynamic-profiles <profile-name> interfaces pp0 unit "$junos-interface-unit" family mlppp service-interface
<si-x> set dynamic-profiles <profile-name> interfaces pp0 unit "$junos-interface-unit" family mlppp
dynamic-profile <ml-profile-name> set dynamic-profiles <profile-name> interfaces
"$junos-interface-ifd-name" unit "$junos-interface-unit" advisory-options upstream-rate
<shaping-rate-in-bps> set dynamic-profiles <profile-name> interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit" advisory-options downstream-rate <shaping-in-bps> set dynamic-profiles
<profile-name> interfaces pp0 unit "$junos-interface-unit" family inet service input service-set
<service-set-name> service-filter <service-filter-name> set dynamic-profiles <profile-name> interfaces
pp0 unit "$junos-interface-unit" family inet service output service-set <service-set-name> service-filter
<service-filter-name> set dynamic-profiles <profile-name> interfaces pp0 unit "$junos-interface-unit"
family inet6 service input service-set <service-set-name> service-filter <service-filter-name> set
dynamic-profiles <profile-name> interfaces pp0 unit "$junos-interface-unit" family inet6 service output
service-set <service-set-name> service-filter <service-filter-name> set dynamic-profiles <profile-name>
interfaces demux0 unit "$junos-interface-unit" family inet service input service-set <service-set-name>
service-filter <service-filter-name> set dynamic-profiles <profile-name> interfaces demux0 unit
"$junos-interface-unit" family inet service output service-set <service-set-name> service-filter
<service-filter-name> set dynamic-profiles <profile-name> interfaces demux0 unit "$junos-interface-unit"
family inet6 service input service-set <service-set-name> service-filter <service-filter-name> set
dynamic-profiles <profile-name> interfaces demux0 unit "$junos-interface-unit" family inet6 service
output service-set <service-set-name> service-filter <service-filter-name> set dynamic-profiles
<profile-name> interfaces pp0 unit "$junos-interface-unit" account-layer2-overhead ingress <bytes>
set dynamic-profiles <profile-name> interfaces pp0 unit "$junos-interface-unit" account-layer2-overhead
egress <bytes> set dynamic-profiles <profile-name> interfaces demux0 unit "$junos-interface-unit"
account-layer2-overhead ingress <bytes> set dynamic-profiles <profile-name> interfaces demux0 unit
"$junos-interface-unit" account-layer2-overhead egress <bytes> set dynamic-profiles <profile-name>
protocols igmp interface "$junos-interface-name" distributed set dynamic-profiles <profile-name>
protocols igmp interface "$junos-interface-name" ssm-map-policy <ssm-map-policy-name> set
dynamic-profiles <policy-name> protocols igmp interface "$junos-interface-name" group-policy
<group-filter-policy-name>.PR1286507

```

- The smg-service process (daemon) might generate a core file in the backup Routing Engine with distributed IGMP configuration. For example, during a subscriber login with multiple service activations, the multicast service gets activated successfully but the login is aborted for other reasons. The backup Routing Engine, which is in the midst of replicating the multicast state, has to abort the login and there is a problem in the cleanup code. [PR1288465](#)
- IPv6 neighbor entries not exported from JTI server. [PR1290777](#)
- This will occur only at corner case where Routing Engine mastership role interpreted differently by RPD and JSR_JSM thread in kernel. [PR1291247](#)
- MX10003 platform does not support "Rescue configuration is not set" alarm. None of the other MX series platforms support this feature. In 17.3R1 release, MX10003 platform checks for rescue configuration file in the system, if the configuration file is not present then this minor alarm is raised. This minor alarm does not have any side-effect and does not cause any other issue with the system operation. This alarm should be ignored on MX10003. [PR1291525](#)
- Some DHCPV4 clients are not coming up during login and logout test. [PR1292582](#)
- Routing Engine get stuck and booted from other SSD post vmhost reboot. [PR1295219](#)
- 3RU:[PTP]: PTP slave is taking longer time (more than 1 hour) to lock to Master in T-BC scenario test. [PR1298792](#)
- Intermittent core is observed in instance scaling and auto-rd configuration when NSR is enabled. The core happens on the primary Routing Engine. [PR1301986](#)

Hardware

- When you plug in or remove an SFP or SFP+ transceiver in any of the supported ports on an MX150, the ge-0/0/0 interface goes down and cannot be used. As a workaround, you can restart the FPC using the request chassis fpc 0 restart command so the ge-0/0/0 interface is up and accessible.

When the MX150 boots up with an SFP or SFP+ transceiver is plugged into any of the supported ports, the status LED for the ge-0/0/0 interface does not glow. However, the ge-/0/0/0 interface can send and receive traffic. The status LED for the ge-0/0/0 interface blinks when traffic is sent or received on this port. [PR1259112](#)

Infrastructure

- After doing graceful Routing Engine switchover on a firewall configuration, you might be unable to log in as the superuser until you log in through the console port. [PR1230657](#)
- In MX10003 platform, last flapped time stamp is not updated when management interface, fxp0, is physically flapped. [PR1244502](#)

- The CLI output of **show system users** displays more users than are actually using the router. The **request system logout** CLI command is unable to clear the stale telnet sessions. This is a cosmetic issue, because **show system connection** and the CLI process show only the current session. [PR1247546](#)
- When **console log-out-on-disconnect** is enabled, system reboot or switchover might result in processes hanging and syslog features failing. [PR1253544](#)

Interfaces and Chassis

- While configuring an aggregated Ethernet interface and after committing, some harmless log messages might appear. The MRU of aggregated Ethernet interface might also reset to the default value (for example, 1522). [PR1261423](#)
- Convergence time for VRRP traffic will be higher if Router or Routing Engine is rebooted in a single Routing Engine system. It is recommended to have a dual Routing Engine system with redundancy enabled. In this case if master Routing Engine is rebooted, backup Routing Engine will take over mastership. There will not be any disruption in VRRP traffic. [PR1270168](#)
- When FPC with both core link and member link of AE (running vrrp) is restarted or offlined convergence time will be higher. [PR1270811](#)
- Junos OS upgrade involving Junos OS Release 14.2R5 and later maintenance releases and Junos OS Release 16.1 and later main releases with CFM configuration might cause CFMD to generate a core file after upgrade. This is due to the old version of `/var/db/cfm.db`. [PR1281073](#)
- Higher MTU configuration on IRB than member link of its VLAN might bring down VRRP session configured on the IRB. To avoid this scenario, always have MTU configured on IRB of VLAN less than or equal to the MTU configured on its member links of same VLAN. [PR1295763](#)

Layer 2 Features

- When the aggregated Ethernet bundle exists in the VPLS routing instance and if the operator incorrectly adds the member link to the same or different instance, the commit will succeed and can cause 100 percent rpd utilization until the incorrect configuration gets manually corrected. This issue occurs because the rpd does not parse the interface configuration, and hence it is not possible to fail the commit. This misconfiguration issue should not have any adverse impact on the device. [PR1280979](#)

MPLS

- Routing protocol daemon (RPD) might stop running unexpectedly if a static MPLS LSP is moved from one routing instance to another routing instance in one single configuration change with one single commit. The rpd will need a manual restart with **restart routing**. [PR1238698](#)
- An LDP egress route that is stitched to a BGP route by means of the **LDP egress-policy** configuration causes the rpd to generate a core file. [PR1290789](#)

Platform and Infrastructure

- On MX Series routers, parity memory errors might occur in pre classifier engines within an MPC. Packets will be silently discarded. Because such errors are not reported, they are more difficult to diagnose. [PR1059137](#)
- 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 broadcast, unicast, and multicast (BUM). As a workaround, nonstop bridging (NSB) can be configured at **[set protocols layer2-control nonstop-bridging]**. This reduces traffic flood to around 10 seconds in a moderate setup. [PR1275621](#)
- Log messages might get triggered when any non-superuser or non-root user tries to telnet into the router. [PR1289974](#)

Routing Protocols

- Few bfd sessions are flapping while coming up after fpc restart/reboot. This does not impact the system as the flap is seen during the bring up phase. This is due to a race condition in PPMAN code. [PR1274941](#)

Services Applications

- Business services are activated and a Routing Engine switchover is performed. In this case, if you try to deactivate the business services (also known as ESSM subscribers) by logging out the parent PPP session, the business services get stuck in terminating state. Business services that have LI applied are stuck, and the services that do not have LI are logged out successfully. [PR1280074](#)
- JL2TP daemon restart should be avoided. GRES followed by jl2tpd daemon restart will result in the loss of subscriber. [PR1293783](#)

VPN

- This issue is applicable only for MX Series routers, PBB-EVPN feature, and Multihome with Active-Active mode. There was a traffic loss when the core link is disabled on DF node. The expected behavior is that the other peer node resumes the DF role and there should not be any traffic loss. [PR1285875](#)

SEE ALSO

[New and Changed Features | 86](#)

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

[Known Behavior | 115](#)

[Resolved Issues | 123](#)[Documentation Updates | 128](#)[Migration, Upgrade, and Downgrade Instructions | 129](#)[Product Compatibility | 136](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 17.3R1 | 123](#)

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

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

Resolved Issues: 17.3R1

Class of Service (CoS)

- The Routing Engine level **scheduler-hierarchy** command misses a forwarding class when the "per-unit-scheduler" mode is configured. [PR1281523](#)

Forwarding and Sampling

- Unexpected messages might be seen in logs. [PR1270686](#)
- The sampled process stops collecting data on Routing Engine based sampling supported platforms. [PR1270723](#)
- The sampled process might crash if traceoptions are enabled. [PR1289530](#)

General Routing

- On MX240/480/960 platforms, due to I2C bus hardware issue, FPC might reboot and error message might appear. [PR1174001](#)
- In MX Series subscriber management environment, the rpd might crash in the backup Routing Engine after executing Routing Engine switch over. [PR1206804](#)
- On MX Series routers with MPC2E-3D-NG/MPC2E-3D-NG-Q/MPC3E-3D-NG/MPC3E-3D-NG-Q line card, if the FPC-MIC link failure happens, the bridge might keep sending register messages in an infinite

loop, which would cause continuous PCI exceptions, the MPC might crash and traffic forwarding might be affected. This is a rare issue, it is hard to reproduce. [PR1231167](#)

- XM chip based line card (MPC3E/4E/5E/6E/2E-NG/3E-NG) might drop traffic under high temperature (67C or higher). [PR1244375](#)
- On MX2000 with MPC6E, EOAM LFM adjacency flaps when an unrelated MIC accommodated in the same MPC6E slot is brought online by configuring OAM pdu-interval 100 ms and pdu-threshold 3. [PR1253102](#)
- When unified ISSU is performed under scaled scenarios where the Packet Forwarding Engine next-hop memory uses more than 4 Million Dwords, PPE traps and traffic loss may be observed during the software-sync phase until the end of the hardware sync. [PR1267680](#)
- The mspmand log messages about memory zone level which should not be generated are generated. It will occur every 49.7 days and will recover by itself. This is a display issue and will not affect the traffic. [PR1273901](#)
- The CLI commands fails for the following commands: **show subscribers detail**, **show subscribers extensive**, **show subscribers count client-type <>**, and other commands. The failure occurs because the subscriber-management database is unavailable. [PR1274464](#)
- Link stays down after a flap on MPC next generation cards with QSFP+-40G direct attach copper (DAC). [PR1275446](#)
- VT interface flaps during unrelated commit operations if MTU is configured on it. [PR1277600](#)
- vlan-oob subscriber session fails in autoconfd due to physical interface down even if the interface is up. [PR1279612](#)
- **MIC Error code: 0x1b0001** alarm was not clear even after the voltage was returned to normal. [PR1280558](#)
- In a subscriber management environment, if authenticated subscriber dynamic VLAN receives idle timeout from the Radius server, due to a rare timing issue such dynamic VLAN interface can be removed immediately after it was successfully created. [PR1280990](#)
- Establishment of IPsec SAs for link type tunnels might fail under certain conditions in case of scaled IPsec link type service set configuration. In such cases the inside IFL corresponding to service set would remain down. This can be resolved by restarting ipsec-key-management daemon by issuing the following command -----8< -----8< ----- restart ipsec-key-management -----8< -----8< ----- Additionally sometimes the traffic may be affected after restarting IPsec management daemon. Clearing IPsec SAs corresponding to such service set would resolve this issue. This can be achieved by running the following commands -----8< -----8< ----- clear services ipsec-vpn ipsec security association <service-set> -----8< -----8< ----- [PR1281223](#) [PR1281223](#)
- DHCP/PPPoE subscribers fail to bind after FPC restart and smgd restart with BBE_RTsock_GET_RTsock_IFL_FAIL_TERMINATED counter going up. [PR1281930](#)
- Inline-JFlow unrelated configuration changes related to a routing-instance results in invalid/incomplete JFlow data packets. Commit-full resumes proper functionality. [PR1282580](#)

- Error messages related to "IFRT: 'IFL'", "IFRT: 'Aggregate interface'" and "IFRT: 'IFD'" seen on config change [PR1282938](#)
- VBF flows are not programmed correctly on aggregated Ethernet interfaces resulting in 50% traffic loss. [PR1282999](#)
- OAM fails to come up when GRE tunnel source and family inet address are the same. [PR1283646](#)
- PPTP session could not be established on MSMPC when it is both stateful-firewall and NAT enabled, and the address could not be translated. [PR1285207](#)
- Possible High CPU on MPC4E when interfaces have been disabled by administrator. [PR1285673](#)
- The J-Flow data template sequence number is zero for MPLS flows. [PR1285975](#)
- Process routing protocol daemon might crash while logging in or logging out with multicast service enabled and performing a GRES switchover. [PR1286653](#)
- L2TP tunnel switch functionality is not working on Junos OS Release 16.1R4-S2 if rewrite-rule configuration is applied to the dynamic profile. [PR1287788](#)
- services-oids-ev-policy.slax & services-oids.slax files built in Junos OS images are not using latest versions. [PR1287894](#)
- After offlining and onlining fabric planes, a few planes are stuck in the offline state in the MX480 router. [PR1287973](#)
- Backup bbe-smgd.core with distributed IGMP configuration. [PR1288465](#)
- If any of the vmhost application is not running then the alarm string will have "Application" name embedded in it. [PR1290150](#)
- BBE-SMGD generates a core file following a stress test in bbe_iff_add_ifa. [PR1291969](#)
- CPCDD might generate core files while using Routing Engine-based http-redirect. [PR1293553](#)
- Not able to edit dynamic profiles after scaling up to 400 dynamic profiles. [PR1295446](#)
- bbe-smgd core at bbe_mcast_ifl_vbf_encoder on service activation or deactivation along with smg-service restarts. [PR1295938](#)

Interfaces and Chassis

- L2TP sessions are not coming up on some of si interfaces after an MPC restart followed by a Routing Engine switchover. [PR1290562](#)

Layer 2 Features

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

Layer 2 Ethernet Services

- DHCP is not using the configured IRB MAC as the source MAC because DHCP is offering only unicast replies. [PR1272618](#)

MPLS

- NG-MVPN MLDP at the receivers' PE does not join P2MP LSP on changing the root PE route from IGP/LDP to LBGp. [PR1277911](#)

Network Management and Monitoring

- The command Esc-q does not work to toggle the console log/terminal log. [PR1269274](#)
- The MIB II process (mib2d) logs an "RLIMIT curr 1048576000 max 1048576000" message every time a commit is performed. [PR1286025](#)
- The mib2d process might crash when polling the OID ifStackStatus.0 after an IFL of lo0 is deleted. [PR1286351](#)

Platform and Infrastructure

- Traffic drop might occur under a large scale of firewall filter configuration. [PR1093275](#)
- FPC crashes with MAC accounting feature enabled. [PR1173530](#)
- FPC CPU spikes every 6 minutes on MX Series routers with MICs and MPCs chipsets due to micro code rebalance. [PR1207532](#)
- RPM loss percent values for "overall tests" through SNMP is incorrect. [PR1272566](#)
- The CLI command **request routing-engine login other-routing-engine** might require a password. [PR1283430](#)
- Transit traffic with DMAC starting with "02" will be punted to Routing Engine when mac-learn-enable is configured. [PR1285874](#)
- The source MAC learned over cross-PFE aggregated Ethernet might bounce between aggregated Ethernet member Packet Forwarding Engines for a long time and which might cause MLP-ADD storm. [PR1290516](#)
- RMOPD might get stuck in the sbwait state upon receiving a specific response from the HTTP agent. [PR1292151](#)

Routing Protocols

- Routing protocol daemon on the backup Routing Engine might restart unexpectedly upon the addition of a new L2VPN routing instance. [PR1233514](#)
- When the **advertise-from-main-vpn-tables** configuration statement is used under BGP and if RR functionality is added, a refresh message is not sent, and as a result, some routes are missed. [PR1254066](#)
- MPLSoUDP tunnel creation failure in the absence of a routing instance table. [PR1270955](#)
- After Routing Engine switchover (GRES+GR) default mdt failed to come up also seen with core facing interface flap. [PR1279459](#)
- Routing protocol daemon might crash due to a certain chain of events in the BGP-LU protection scenario. [PR1282672](#)
- The second multicast packet might be discarded on RP router. [PR1282848](#)
- Routing protocol daemon crashes while deactivating in a routing instance protocols pim static. [PR1284760](#)
- Routing protocol daemon might crash if dynamic RP goes down in ECMP topology when PIM join load balancing automatic is configured. [PR1288316](#)

Services Applications

- DTCP LI filters are very slow to program when using the "X-RM-Circuit-ID" trigger. [PR1269770](#)
- Business service fails to get deactivated post Routing Engine switchover. [PR1280074](#)
- Backup Routing Engine is going to the database prompt with a vmcore if the down ASI interface configuration is deleted. [PR1281882](#)
- Loss of all L2TP subscribers on an LAC router after smg-service restarts on the L2TP tunnel switch.. [PR1284260](#)
- The l2tpd process generates a core file with reference to 0x084166f5 in L2tpTunnel::createSucceeded (this=0xa04ae84, createFlags=...) at ../src/junos/usr.sbin/jl2tpd/l2tpTunnel.cc:1845. [PR1288029](#)
- Each subscriber session is getting its own L2TP tunnel without "Tunnel-Client-Endpoint" from radius. [PR1293927](#)

Subscriber Management and Services

- MX Series router could not filter some RADIUS attributes with the accounting-Off and accounting-On messages. [PR1279533](#)
- Authenticated subscriber dynamic VLAN interface might get disconnected immediately after a successful connection. [PR1280990](#)
- Authd core file is observed while terminating large number of subscribers. [PR1289215](#)

User Interface and Configuration

- The commitd process might generate a core file by certain configuration removal followed by a commit operation. [PR1267433](#)

VPNs

- Routing protocol daemon memory leak is observed in next-generation-MVPN enviroment. [PR1259579](#)

SEE ALSO

New and Changed Features 86
Changes in Behavior and Syntax 110
Known Behavior 115
Known Issues 116
Documentation Updates 128
Migration, Upgrade, and Downgrade Instructions 129
Product Compatibility 136

Documentation Updates

IN THIS SECTION

- [Subscriber Management Provisioning Guide | 129](#)

This section lists the errata and changes in Junos OS Release 17.3R1 documentation for MX Series.

Subscriber Management Provisioning Guide

- The *Broadband Subscriber Sessions User Guide* did not report that you can suspend AAA accounting, establish a baseline of accounting statistics, and resume accounting. This feature was introduced in Junos OS Release 15.1R4.

[See [Suspending AAA Accounting and Baseline Accounting Statistics Overview](#).]

SEE ALSO

[New and Changed Features | 86](#)

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

[Known Behavior | 115](#)

[Known Issues | 116](#)

[Resolved Issues | 123](#)

[Migration, Upgrade, and Downgrade Instructions | 129](#)

[Product Compatibility | 136](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading to Release 17.3 | 130](#)
- [Procedure to Upgrade to FreeBSD 10.x based Junos OS | 131](#)
- [Procedure to Upgrade to FreeBSD 6.x based Junos OS | 133](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 134](#)
- [Upgrading a Router with Redundant Routing Engines | 135](#)
- [Downgrading from Release 17.3 | 135](#)

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

Starting with Junos OS Release 15.1, in some of the devices, FreeBSD 10.x is the underlying OS for Junos OS instead of FreeBSD 6.x. This feature includes a simplified package naming system that drops the domestic and world-wide naming convention. However, in some of the routers, FreeBSD 6.x remains the underlying OS for Junos OS. For more details about FreeBSD 10.x, see [Understanding Junos OS with Upgraded FreeBSD](#).

NOTE: In Junos OS Release 15.1, Junos OS (FreeBSD 10.x) is not available to customers in Belarus, Kazakhstan, and Russia. Customers in these countries need to use the existing Junos OS (FreeBSD 6.1).

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

Platform	FreeBSD 6.x-based Junos OS	FreeBSD 10.x-based Junos OS
MX80, MX104	YES	NO
MX240, MX480, MX960, MX2010, MX2020	NO	YES

Basic Procedure for Upgrading to Release 17.3

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

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

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

For more information about the installation process, see [Installation and Upgrade Guide](#) and [Upgrading Junos OS with Upgraded FreeBSD](#).

Procedure to Upgrade to FreeBSD 10.x based Junos OS

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

To download and install FreeBSD 10.x based Junos OS:

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot  
source/junos-install-mx-x86-32-17.3R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-64-17.3R1.9-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the **junos-vmhost-install-x.tgz** image and specify the name of the regular package in the **request vmhost software add** command. For more information, see VM Host Installation topic in the [Installation and Upgrade Guide](#).

NOTE: After you install a Junos OS Release 17.3**jinstall** package, you cannot return to the previously installed Junos OS (FreeBSD 6.1) software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add no-validate** command and specify the **jinstall** package that corresponds to the previously installed software.

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

Procedure to Upgrade to FreeBSD 6.x based Junos OS

Products impacted: MX80, and MX104.

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

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

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

```
user@host> request system software add validate reboot  
source/jinstall-17.3R1.9-domestic-signed.tgz
```

- All other customers, use the following command:

```
user@host> request system software add validate reboot source/jinstall-17.3R1.9-export-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 17.3 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 16.2, 17.1 and 17.2 are EEOL releases. You can upgrade from Junos OS Release 16.2 to Release 17.1 or even from Junos OS Release 16.2 to Release 17.2. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

For more information about EEOL releases and to review a list of EEOL releases, see <https://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 17.3

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

NOTE: You cannot downgrade more than three releases.

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

SEE ALSO

[New and Changed Features | 86](#)

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

[Known Behavior | 115](#)

[Known Issues | 116](#)

[Resolved Issues | 123](#)

[Documentation Updates | 128](#)

[Product Compatibility | 136](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 136](#)

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 | 86](#)

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

[Known Behavior | 115](#)

[Known Issues | 116](#)

[Resolved Issues | 123](#)

[Documentation Updates | 128](#)

[Migration, Upgrade, and Downgrade Instructions | 129](#)

Junos OS Release Notes for NFX Series

IN THIS SECTION

- New and Changed Features | 137
- Changes in Behavior and Syntax | 138
- Known Behavior | 139
- Known Issues | 139
- Resolved Issues | 140
- Documentation Updates | 140
- Migration, Upgrade, and Downgrade Instructions | 141
- Product Compatibility | 142

These release notes accompany Junos OS Release 17.3R1 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

- Juniper Device Manager | 138

This section describes the new features or enhancements to existing features in Junos OS Release 17.3R1 for NFX Series.

Juniper Device Manager

- **Support for Virtual Route Reflector (NFX250-S2)**—Starting in Junos OS Release 17.3R1, you can implement the virtual router reflector capability by creating and deploying a VRR virtual machine as a VNF (Virtual Network Function) on the NFX250-S2 device. Benefits of implementing virtual route reflectors are:
 - Improved scalability
 - Fast and more flexible deployment
 - Savings as a result of elimination of router hardware

SEE ALSO

Changes in Behavior and Syntax 138
Known Behavior 139
Known Issues 139
Resolved Issues 140
Documentation Updates 140
Migration, Upgrade, and Downgrade Instructions 141
Product Compatibility 142

Changes in Behavior and Syntax

There are no changes in behavior and syntax for NFX Series in Junos OS Release 17.3R1

SEE ALSO

New and Changed Features 137
Known Behavior 139
Known Issues 139
Resolved Issues 140
Documentation Updates 140
Migration, Upgrade, and Downgrade Instructions 141
Product Compatibility 142

Known Behavior

There are no known limitations in Junos OS Release 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.

SEE ALSO

New and Changed Features 137
Changes in Behavior and Syntax 138
Known Issues 139
Resolved Issues 140
Documentation Updates 140
Migration, Upgrade, and Downgrade Instructions 141
Product Compatibility 142

Known Issues

There are no known issues in hardware and software in Junos OS Release 17.3R1 for NFX Series.

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

SEE ALSO

New and Changed Features 137
Changes in Behavior and Syntax 138
Known Behavior 139
Resolved Issues 140
Documentation Updates 140
Migration, Upgrade, and Downgrade Instructions 141
Product Compatibility 142

Resolved Issues

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

SEE ALSO

New and Changed Features 137
Changes in Behavior and Syntax 138
Known Behavior 139
Documentation Updates 140
Known Issues 139
Migration, Upgrade, and Downgrade Instructions 141
Product Compatibility 142

Documentation Updates

There are no errata or changes in Junos OS Release 17.3R1 documentation for NFX Series.

SEE ALSO

New and Changed Features 137
Changes in Behavior and Syntax 138
Known Behavior 139
Known Issues 139
Resolved Issues 140
Migration, Upgrade, and Downgrade Instructions 141
Product Compatibility 142

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 141](#)

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or even from Junos OS Release 14.1 to Release 16.1. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

SEE ALSO

[New and Changed Features | 137](#)

[Changes in Behavior and Syntax | 138](#)

[Known Behavior | 139](#)

[Documentation Updates | 140](#)

[Known Issues | 139](#)

Resolved Issues 140
Product Compatibility 142

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 142

Hardware Compatibility

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

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

Hardware Compatibility Tool

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

SEE ALSO

New and Changed Features 137
Changes in Behavior and Syntax 138
Known Behavior 139
Documentation Updates 140
Known Issues 139
Resolved Issues 140
Migration, Upgrade, and Downgrade Instructions 141

Junos OS Release Notes for PTX Series Packet Transport Routers

IN THIS SECTION

- New and Changed Features | 143
- Changes in Behavior and Syntax | 151
- Known Behavior | 154
- Known Issues | 155
- Resolved Issues | 157
- Documentation Updates | 158
- Migration, Upgrade, and Downgrade Instructions | 158
- Product Compatibility | 163

These release notes accompany Junos OS Release 17.3R1 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- Class of Service | 144
- General Routing | 145
- Interfaces and Chassis | 145
- Management | 146
- Multicast | 147
- Network Management and Monitoring | 148
- Operation, Administration, and Maintenance | 148
- Routing Policy and Firewall Filters | 149

- Routing Protocols | 150
- Services Applications | 151

This section describes the new features and enhancements to existing features in Junos OS Release 17.3R1 for the PTX Series.

Class of Service

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

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

- **Support for shaping of the traffic exiting a physical interface (PTX10008)**—Starting with Junos OS Release 17.3R1, you can shape the output traffic of a physical interface on PTX10008 routers so that the interface transmits less traffic than it is physically capable of carrying. Shaping on a PTX10008 router interface has a minimum rate of 1 Gbps and an incremental granularity of 0.1 percent of the physical interface speed after that (for example, 10 Mbps increments on a 10 Gbps interface). You can shape the output traffic of a physical interface by including the **shaping-rate** statement at the **[edit class-of-service interfaces interface-name]** or **[edit class-of-service traffic-control-profiles profile-name]** hierarchy level and applying the traffic control profile to an interface.

[See [shaping-rate \(Applying to an Interface\)](#).]

General Routing

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

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

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

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

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

Interfaces and Chassis

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

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

- **Support for confining management Ethernet Interface (fxp0) in a virtual routing and forwarding table (PTX10008)**—Starting in Junos OS Release 17.3R1, Junos OS is able to confine the management interface in a dedicated management instance by setting a new CLI configuration statement, **management-instance**, at the **[edit system]** hierarchy level. By doing so, operators will ensure that management traffic no longer has to share a routing table (that is, default.inet.0 table) with other control or protocol traffic in the system. Instead, there is a **mgmt_junos** routing instance introduced for management traffic.

For more information, see [Configuring the mgmt_junos Routing Instance](#)

Management

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

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

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

/network-instances/network-instance/[name_ 'instance-name']/protocols/protocol/

Additionally, the following paths are also now supported:

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

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

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

- **Junos Telemetry Interface support for Routing and Control Board RCB-PTX-X6-32G (PTX3000)**—Starting with Junos OS Release 17.3R1, the Routing and Control Board (RCB) on PTX3000 routers supports the Junos Telemetry Interface, which enables you to provision sensors to export telemetry data for various network elements. The RCB combines the functionality of a Routing Engine, Control Board, and Centralized Clock Generator (CCG) in a single FRU. To provision sensors to stream data through UDP,

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

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

- **Enhanced support for Junos Telemetry Interface (PTX1000 routers)**—Starting with Junos OS Release 17.3R1, you can also provision sensors through the Junos Telemetry Interface for the following network elements:
 - Logical interfaces, including queue statistics (UDP and gRPC streaming)
 - BGP Peers (gRPC streaming only)
 - Memory utilization for routing protocol tasks (gRPC streaming only)
 - RSVP interface events (gRPC streaming only)
 - Firewall filters, including traffic-class counter (UDP and gRPC streaming)
 - Chassis components (gRPC streaming only)
 - Aggregated Ethernet interfaces configured with the Link Aggregation Control Protocol (gRPC streaming only)
 - Ethernet interfaces enabled configured with the Link Layer Discovery Protocol (gRPC streaming only)
 - Routing Engine logical and physical interfaces (UDP and gRPC streaming)
 - Optical interfaces (UDP and gRPC streaming)
 - Network Discovery Protocol table state (gRPC streaming only)
 - Address Resolution Protocol table state (gRPC streaming only)
 - IPFIX inline flow aggregation (UDP streaming only)

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

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

Multicast

- **Support for next generation MVPN and Internet multicast (PTX1000)**—Starting in Junos OS Release 17.3R1, the **mpls-internet-multicast** routing instance type uses ingress replication provider tunnels to carry IP multicast data between routers through an MPLS cloud, using MBGP (or next generation) MVPN.

NOTE: Next-generation MVPN is supported only when the **enhanced-mode** statement is configured at the **[edit chassis network-services]** hierarchy level.

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

- **Support for next generation MVPN and Internet multicast (PTX10008)**—Starting in Junos OS Release 17.3R1, the **mpls-internet-multicast** routing instance type uses ingress replication provider tunnels to carry IP multicast data between routers through an MPLS cloud, using MBGP (or next generation) MVPN. Next generation MVPN is available only for PTX Series routers that have third-generation FPCs installed.

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

Network Management and Monitoring

- **mLDP MIB extends support to LDP point-to-multipoint (P2MP) LSPs (PTX Series)**—Starting in Junos OS Release 17.3R1, the mLDP MIB builds on the objects and tables that are defined in RFC 3815, which only support LDP point-to-point label switched paths (LSPs). This mLDP MIB provides support for managing multicast LDP point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) LSPs. The mLDP MIB tables are directly accessible through SNMP. All objects in the mLDP MIB are read-only and cannot be created or set through SNMP. This implementation of mLDP MIB is specified in draft-ietf-mpls-mldp-mib.
- **Support for inline jflow version 9 flow templates (PTX1000)**—Starting in Junos OS Release 17.3R1, you can use inline-JFlow's export capabilities with version 9 flow templates to define a flow record template suitable for IPv4 or IPv6 traffic.

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

Operation, Administration, and Maintenance

- **Junos OS daemons to natively emit JSON output (PTX Series)**—Starting with Junos OS Release 17.3R1, the operational state emitted by the daemons is supported in JSON format as well as XML format. To configure JSON format, specify the following CLI command: **set system export-format state-data json compact**. To specify JSON format for specific command output, include **display json** in specific CLI commands.
- **Junos OS OpenConfig to support adjacent RIB operational state model (PTX Series)**—Starting with Junos OS Release 17.3R1, **adj-rib-in-pre** and **adj-rib-out-post** tables have been added for the OpenConfig RIB operational state mode. The BGP RIB consists of several tables per address family, consisting of **loc-rib** and per-neighbor tables.

Routing Policy and Firewall Filters

- **Optimized performance for DSCP and traffic-class firewall filter match conditions (PTX10008)**—Starting in Junos OS Release 17.3R1, the **promote dscp** and **promote traffic-class** indicators are supported in firewall filters for IPv4 and IPv6 traffic. When either of these are applied to a filter, the entire filter is compiled in a way that optimizes its performance for the **dscp** or **traffic-class** match condition. The indicators are configured at the **[edit firewall family (inet | inet6) filter filter-name]** hierarchy level.

NOTE: Enabling the indicators requires that network services is set to **enhanced-mode**. Use of the indicators may impact the performance of the **source-port** match condition.

- **Optimized performance for DSCP and traffic-class firewall filter match conditions (PTX1000)**—Starting in Junos OS Release 17.3R1, the **promote dscp** and **promote traffic-class** indicators are supported in firewall filters for IPv4 and IPv6 traffic. When either are applied to a filter, the entire filter is compiled in a way that optimizes its performance for the **dscp** or **traffic-class** match condition. The indicators are configured at the **[edit firewall family (inet | inet6) filter filter-name]** hierarchy level.

NOTE: Enabling the indicators requires that network services be set to **enhanced-mode**. Use of the indicators might impact the performance of the **source-port** match condition.

[See [Promote DSCP](#) and [Promote traffic-class](#).]

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

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

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

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

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

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

Routing Protocols

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

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

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

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

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

- **Support for BGP Large Communities (PTX Series)**—Starting with Junos OS Release 17.3R1, BGP community is enhanced to support BGP large community that uses 12-byte encoding where the most significant 4 bytes encode autonomous system number or global administrator and the remaining two 4 bytes encode operator defined local values. Currently, BGP normal community (4 byte) and BGP extended community (6 byte) provide limited support for BGP community attributes after the introduction of 4-byte autonomous system number. Configure the large BGP community attributes at the **[edit policy-options community *community-name* members]** hierarchy level and at the **[edit routing-options static route *route* community]** hierarchy level with keyword **large** followed by three 4-byte unsigned

integers separated by colons. The attributes are represented as large:autonomous system number:local value 1:local value2.

- **Support for BGP to carry flow-specification routes (PTX10008)**—Starting in Junos OS Release 17.3R1, BGP can carry flow-specification network layer reachability information (NLRI) messages on a PTX10008 router. Propagating firewall filter information as part of BGP enables you to propagate firewall filters against denial-of-service (DoS) attacks dynamically across autonomous systems.

[See [Example: Enabling BGP to Carry Flow-Specification Routes.](#)]

Services Applications

- **Support for inline JFlow version 9 flow templates (PTX 10008 routers)**—Starting in Junos OS Release 17.3R1, you can use inline-JFlow export capabilities with version 9 flow templates to define a flow record template suitable for IPv4 or IPv6 traffic.

[See [Monitoring Network Traffic Flow Using Inline Flow Monitoring on PTX Series Routers.](#)]

SEE ALSO

[Changes in Behavior and Syntax | 151](#)

[Known Behavior | 154](#)

[Known Issues | 155](#)

[Resolved Issues | 157](#)

[Documentation Updates | 158](#)

[Migration, Upgrade, and Downgrade Instructions | 158](#)

[Product Compatibility | 163](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [Forwarding and Sampling | 152](#)
- [General Routing | 152](#)
- [Interfaces and Chassis | 152](#)
- [Management | 152](#)
- [Network Management and Monitoring | 153](#)

- Services Application | 153
- VLAN-Infrastructure | 154

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 17.3R1 for the PTX Series.

Forwarding and Sampling

- In Junos OS Release 17.3R1, and later, the **SelectorID** field (element id: 302) is sent instead of the **Bytes** field (element id: 1) in the system scope of **version-ipfix** Option template records for all PTX Series Routers. All other elements of the template remain the same.

General Routing

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

Interfaces and Chassis

- **Restart FPC option supported on PTX1000 router**—In Junos OS Release 17.3, you can reboot the FPC gracefully using **request chassis fpc restart slot slot-number** command on a PTX1000 router. Note that **request chassis fpc (online|offline) slot slot-number** command is not supported, which means only restart option is supported, but online and offline options are not supported.

[See [request chassis fpc](#).]

Management

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

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

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

Network Management and Monitoring

- **SNMP syslog messages changed (PTX Series)**—In Junos OS Release 17.3R1, two misleading SNMP syslog messages have been rewritten to accurately describe the event:
 - OLD --AgentX master agent failed to respond to ping. Attempting to re-register
NEW -- AgentX master agent failed to respond to ping, triggering cleanup!
 - OLD -- NET-SNMP version %s AgentX subagent connected
NEW --- NET-SNMP version %s AgentX subagent Open-Sent!
- **Enhancement to about-to-expire logic for license expiry syslog messages (PTX Series)**—Starting in Junos OS Release 17.3R1, the logic for multiple capacity type licenses and when their expiry raises alarms was changed. Before, the behavior had alarms and syslog messages for expiring licenses raised based on the highest validity, which would mislead users in the case of a license expiring earlier than the highest validity license. The new behavior has the about-to-expire logic based on the first expiring license.

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

Services Application

- **Changes to the show services rpm history-results command (PTX Series)**—Starting in Junos OS Release 17.3R1, you must include the **owner owner** and **test name** options when using the **show services rpm history-results** command.
- In Junos OS Release 17.3R1 and later, for PIC-based J-Flow on MX Series routers and inline J-Flow on PTX Series routers, the Options template and Options data records include the **Sampling Interval** field as part of the **ScopeTemplate** field instead of the **ScopeSystem** field.

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

VLAN-Infrastructure

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

SEE ALSO

[New and Changed Features | 143](#)

[Known Behavior | 154](#)

[Known Issues | 155](#)

[Resolved Issues | 157](#)

[Documentation Updates | 158](#)

[Migration, Upgrade, and Downgrade Instructions | 158](#)

[Product Compatibility | 163](#)

Known Behavior

There are no known limitations in Junos OS Release 17.3R1 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.

SEE ALSO

[New and Changed Features | 143](#)

[Changes in Behavior and Syntax | 151](#)

[Known Issues | 155](#)

[Resolved Issues | 157](#)

[Documentation Updates | 158](#)

[Migration, Upgrade, and Downgrade Instructions | 158](#)

[Product Compatibility | 163](#)

Known Issues

IN THIS SECTION

- General Routing | [155](#)
- Infrastructure | [156](#)
- Interfaces and Chassis | [156](#)
- Platform and Infrastructure | [156](#)
- Routing Protocols | [156](#)

This section lists the known issues in hardware and software in Junos OS Release 17.3R1 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

- Uneven load balancing of traffic might occur if the traffic stream changes only in the bits 0-15 of the Layer 3 destination IPv6 address. This limitation might not be visible if the other parameters affecting the load balance change along with L3_DST, such as L3 source IP address, L4 source/destination ports, and so on. [PR1065515](#)
- PTX Series FPC3 might receive noise on the FPC console port, and interprets the noise as a valid signal. This might cause the login to fail on the console port, to generate core files, or even to reload. [PR1224820](#)
- On rare occasions, upon reboot, the kernel cannot create sysfs entries for the SSDs in the system. This might result in the system entering panic mode and to hang. [PR1261068](#)
- When you offline/restart an FPC 'x' that is sending traffic to FPC 'y', the following error messages are seen on the destination FPC.

```
Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Error (0x210613), module: PE Chip, type:
Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Cmerror Op Set: PE Chip: PE1[1]: FO:core
intr: 0x00000010: Grant spray drop due to unspray-able condition error
Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Error (0x210614), module: PE Chip, type:
Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Cmerror Op Set: PE Chip: PE1[1]: FO:core
intr: 0x00000008: Request spray drop due to unspray-able condition error
```

- It also results in a corresponding alarm being set on a destination FPC.

- Specific to PTX10000 is the transient alarm that gets set when this condition occurs by CMERROR infra.
- The alarm clears off later because the source FPC is being offlined.

[PR1268678](#)

- Sometimes you can notice l2cpd core files generated when Link Layer Discovery Protocol (lldp) neighbors are cleared. [PR1270180](#)
- With non enhanced-mode, traffic loss is seen on version 4 static-lsp with stitch operation, which does not work on PTX Series routers. [PR1290942](#)
- When downgrading from Junos OS Release 17.3R1 to Junos OS Release 16.1X65, mgd.core will be created if the no-validate option is not used with the software downgrade command. [PR1296504](#)

Infrastructure

- The CLI output of **show system users** displays more users who are not using the router. The **request system logout** CLI command is unable to clear the stale telnet sessions. This is a cosmetic issue, because **show system connection** and the CLI process show only the current session. [PR1247546](#)

Interfaces and Chassis

- After graceful Routing Engine switchover, LFM discovery state for aggregate interface might show up as fault instead of Send Any. This does not affect LFM protocol functionality in any way as LFM protocol always run on physical/member interfaces. The only information conveyed by Send Any state of aggregate interface is that, atleast one member interface has discovery state Send Any. [PR1299534](#)

Platform and Infrastructure

- On PTX Series routers, parity memory errors might happen in preclassifier engines within an MPC. Such errors are not reported, and they are harder to diagnose. CM-ERRORs, such as syslogs and alarms, should be raised when parity memory errors occur. [PR1059137](#)

Routing Protocols

- Few bfd sessions are flapping while coming up after fpc restart/reboot. This doesn't impact the system as the flap is seen during the bring up phase. This is due to a race condition in PPMAN code. [PR1274941](#)

SEE ALSO

New and Changed Features	143
Changes in Behavior and Syntax	151
Known Behavior	154
Resolved Issues	157
Documentation Updates	158
Migration, Upgrade, and Downgrade Instructions	158
Product Compatibility	163

Resolved Issues

IN THIS SECTION

- Resolved Issues: 17.3R1 | 157

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

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

Resolved Issues: 17.3R1

Layer 2 Features

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

SEE ALSO

New and Changed Features	143
Changes in Behavior and Syntax	151
Known Behavior	154
Known Issues	155
Documentation Updates	158
Migration, Upgrade, and Downgrade Instructions	158

Documentation Updates

There are no errata or changes in Junos OS Release 17.3R1 documentation for PTX Series.

SEE ALSO

New and Changed Features 143
Changes in Behavior and Syntax 151
Known Behavior 154
Known Issues 155
Resolved Issues 157
Migration, Upgrade, and Downgrade Instructions 158
Product Compatibility 163

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases | 158
- Upgrading a Router with Redundant Routing Engines | 159
- Basic Procedure for Upgrading to Release 17.3 | 159

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

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases

provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 14.1, 14.2, 15.1 and 16.1 are EEOL releases. You can upgrade from Junos OS Release 14.1 to Release 15.1 or from Junos OS Release 14.2 to Release 16.1. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

For more information about EEOL releases and to review a list of EEOL releases, see <https://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 active as the backup Routing Engine.

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

Basic Procedure for Upgrading to Release 17.3

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

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

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

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

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

To download and install Junos OS Release 17.3R1:

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

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

NOTE: After you install a Junos OS Release 17.3R1 jinstall package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the jinstall package that corresponds to the previously installed software.

The **validate** option validates the software package against the current configuration as a prerequisite to adding the software package to ensure that the router reboots successfully. This is the default behavior when the software package being added is for a different release. Adding the **reboot** command reboots the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process might take 5 to 10 minutes. Rebooting occurs only if the upgrade is successful.

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

```
user@host> request system software add validate reboot source/jinstall-17.3
R1.SPIN-domestic-signed.tgz
```

All other customers, use the following command:

```
user@host> request system software add validate reboot source/jinstall-17.3
R1.SPIN-export-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

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

NOTE: After you install a Junos OS Release 17.3 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

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

SEE ALSO

New and Changed Features	143
Changes in Behavior and Syntax	151
Known Behavior	154
Known Issues	155
Resolved Issues	157
Documentation Updates	158
Product Compatibility	163

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 163](#)

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 | 143](#)

[Changes in Behavior and Syntax | 151](#)

[Known Behavior | 154](#)

[Known Issues | 155](#)

[Resolved Issues | 157](#)

[Documentation Updates | 158](#)

[Migration, Upgrade, and Downgrade Instructions | 158](#)

Junos OS Release Notes for the QFX Series

IN THIS SECTION

- New and Changed Features | 164
- Changes in Behavior and Syntax | 179
- Known Behavior | 181
- Known Issues | 183
- Resolved Issues | 187
- Documentation Updates | 189
- Migration, Upgrade, and Downgrade Instructions | 190
- Product Compatibility | 203

These release notes accompany Junos OS Release 17.3R1 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- Class of Service (CoS) | 166
- EVPNs | 166
- General Routing | 168
- High Availability (HA) and Resiliency | 168
- Interfaces and Chassis | 168
- Layer 2 Features | 170
- Management | 170
- Multicast | 173
- Multiprotocol Label Switching (MPLS) | 173

- Network Management and Monitoring | 174
- Operation, Administration, and Maintenance | 174
- Port Security | 174
- Routing Protocols Policy and Firewall Filters | 175
- Routing Protocols | 175
- Virtual Chassis | 178

This section describes the new features for the QFX Series switches in Junos OS Release 17.3R1.

NOTE: The following QFX Series platforms are supported in Release 17.3R1: QFX5100, QFX5110, QFX5200, QFX10002, QFX10008, and QFX10016.

Class of Service (CoS)

- **Enhanced Transmission Selection (ETS) support (QFX10000 Series)**—Beginning with Junos OS Release 17.3R1, ETS is supported on QFX10000 Series devices, compliant with IEEE 802.1Qaz/D0.1. ETS support enables the definition of multiple priority groups at each egress port of the device. Priority queues are combined into priority groups, enabling the application of similar congestion control capabilities to all queues within a group.

[See [Understanding CoS Hierarchical Port Scheduling \(ETS\)](#).]

EVPNs

- **Support of Layer 3 connectivity in an EVPN-VXLAN topology (QFX5110)**—Starting with Junos OS Release 17.3R1, you can deploy a QFX5110 switch as a Layer 3 Virtual Extensible LAN (VXLAN) gateway in an EVPN-VXLAN topology with a two-layer IP fabric or an IP fabric that is collapsed to one layer. In this role, the QFX5110 switch provides Layer 3 connectivity between physical (bare-metal) servers and virtual machines (VMs) within a data center. On QFX5110 switches, you can configure integrated routing and bridging (IRB) interfaces that route packets between VLANs. While creating an IRB interface, you can configure the interface as a default Layer 3 gateway, which physical servers in one VLAN use to communicate with physical servers or VMs in another VLAN.

[See [Example: Configuring a QFX5110 Switch as a Layer 3 VXLAN Gateway in an EVPN-VXLAN Topology with a Two-Layer IP Fabric](#) and [Example: Configuring a QFX5110 Switch as Layer 2 and 3 VXLAN Gateways in an EVPN-VXLAN Topology with a Collapsed IP Fabric](#).]

- **Support for multiple routing instances of type Virtual Switch and EVPN, VLAN-based service on the EVPN routing instance, and VLAN-aware service on the Virtual Switch routing instance (QFX10000 Series switches)**—Starting with Junos OS Release 17.3R1, you can configure both EVPN and Virtual Switch routing instances. The EVPN routing instance supports VLAN-based service. With VLAN-based service, the EVPN instance includes only a single broadcast domain, and there is a one-to-one mapping between a VNI and MAC-VRF. Up to 100 EVPN routing instances are supported. The Virtual Switch routing instance supports VLAN-aware service, and up to 10 Virtual Switch routing instances with 2000 VLANs are supported.

NOTE: If you create VLANs that are not part of a routing instance, they become part of the Default Switch routing instance.

- **EVPN Proxy ARP and ARP Suppression (QFX10000 switches)**—Starting with Junos OS Release 17.3R1, QFX10000 switches that function as provider edge (PE) devices in an Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) environment support proxy Address Resolution Protocol (ARP) and ARP suppression. The proxy ARP and ARP suppression capabilities are enabled by default. For both features to work properly, the configuration of an integrated and routing (IRB) interface on the PE device is required.

IRB interfaces configured on a PE device deliver ARP requests from both local and remote customer edge (CE) devices. When a PE device receives an ARP request from a CE device, the PE device searches its media access control (MAC)-IP address bindings database for the requested IP address. If the PE device finds the MAC-IP address binding in its database, it responds to the request. If the device does not find the MAC-IP address binding, it swaps the source MAC address in the request with the MAC address of the IRB interface on which the request was received and sends the request to all interfaces.

Even when a PE device responds to an ARP request, ARP packets might still be flooded across the WAN. ARP suppression prevents this flooding from occurring.

[See [EVPN Proxy ARP and ARP Suppression](#).]

- **Support for external multicast router for EVPN with IGMP snooping (QFX10000)**—Starting with Junos OS Release 17.3R1, you can configure a provider edge (PE) switch running Ethernet VPN (EVPN) to send and receive multicast traffic to an external multicast router. This implementation supports the forwarding of inter-VLAN multicast traffic without having to configure IRB interfaces. Traffic is forwarded through a Layer 3 multicast protocol such as Protocol Independent Multicast (PIM). To enable the PE switch to receive multicast traffic from the multicast router, include the **multicast-router-interface** statement at the **[edit protocols igmp-snooping vlan *vlan-name* interface *interface-name*]** hierarchy level.

Support for forwarding inter-VLAN and intra-VLAN multicast traffic in an EVPN-VXLAN environment with IRB interfaces was introduced on QFX10000 switches in Junos OS Release 17.2R1.

[See [multicast-router-interface \(IGMP Snooping\)](#).]

- **Support for external Layer 3 multicast device for EVPN with IGMP snooping (QFX10000)**—Starting with Junos OS Release 17.3R1, you can connect an Ethernet VPN (EVPN) provider edge switch to an external Layer 3 device running a multicast protocol such as Protocol Independent Multicast (PIM). In this implementation, one or more provider edge switches configured with EVPN are connected to an external, that is, gateway, multicast device through a Layer 2 VLAN. To enable the PEs to forward traffic to the external domain, configure PIM-to-IGMP translation by including the **pim-to-igmp-proxy upstream-interface *irb-interface-name*** statements at the **[edit routing-options multicast]** hierarchy level. Additionally, this implementation supports configuring PIM on the IRB interfaces on the PE so that it functions only to forward inter-VLAN traffic within the data center. This means that you do not need to configure a PIM rendezvous point because forming PIM adjacencies is not required. The gateway device only needs to view the data center as a Layer 2 multicast domain. Include the new **passive** statement at the **[edit protocols pim]** hierarchy level to configure PIM to perform only inter-VLAN forwarding of multicast traffic.

[See [Overview of IGMP Snooping in an EVPN-VXLAN Environment](#).]

General Routing

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

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

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

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

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

High Availability (HA) and Resiliency

- **Support for VRRP over IRB interfaces (QFX5100 Virtual Chassis and Virtual Chassis Fabric)**—Starting in Junos OS Release 17.3R1, you can configure Virtual Router Redundancy Protocol Version 3 (VRRPv3) for an IPv4 or IPv6 IRB interface on a QFX5100 Virtual Chassis or Virtual Chassis Fabric (VCF). The Virtual Chassis or VCF can act as the master or backup switch in a VRRP group, and the IRB interface forwards traffic sent to the configured VRRP virtual address that corresponds to the default gateway for the VLAN. Use the **vrrp-group** or **vrrp-inet6-group** configuration statement in the [edit interfaces irb unit *logical-unit-number* family (inet | inet6) address *address*] statement hierarchy on the Virtual Chassis or VCF as part of the IRB interface configuration.

[See [Configuring Basic VRRP Support for QFX](#) and [Configuring IRB Interfaces](#).]

Interfaces and Chassis

- **Increased number of link aggregation groups (LAGs) (QFX10008 and QFX10016 switches)**—Starting with Junos OS Release 17.3R1, you can configure up to 1000 LAGs on QFX10008 and QFX10016 switches. To configure, include the **device-count** statement with a value of 1000 at the [edit chassis aggregated-devices ethernet] hierarchy level and add member links in each bundle.
- **Short-reach mode (QFX5100-48T switch)**—Allows you to use short cable lengths (less than 10 meters) for copper-based 10-Gigabit Ethernet interfaces. Enabling short-reach mode reduces power consumption on these interfaces. You can configure short-reach mode for individual interfaces and for a range of interfaces. Enable short-reach mode for individual interfaces by including the enable statement at the [edit chassis fpc <slot-number> pic <slot-number>] hierarchy. Enable short-reach mode for a range of

interfaces by including the enable statement at the `[edit chassis fpc <slot-number> pic port-range <port low> <port high>]` hierarchy.

- **IEEE 1588v2 Precision Time Protocol (PTP) Boundary Clock (QFX10002 switches)**—Starting with Junos OS Release 17.3R1, a boundary clock, which has multiple network connections, can act as a source (master) or destination (slave) for synchronization messages. The boundary clock intercepts and processes all Precision Time Protocol (PTP) messages and passes all other traffic. The best master clock algorithm (BMCA) is used by the boundary clock to select the best clock from configured acceptable masters. You can configure a port as a boundary slave or as a boundary master. To configure a boundary clock, include the **boundary** statement at the `[edit protocols ptp clock-mode]` hierarchy level.

[See [IEEE 1588v2 PTP Boundary Clock Overview](#).]

- **Auto-channelization of interfaces (QFX5200 switch)**—Starting in Junos OS Release 17.3, you can use the auto-channelization feature to divide and channelize data automatically by detecting the cable type. The mode and number of channels are decided based on the channel link status. On QFX5200, auto-channelization supports three modes of operation with unique port settings:
 - When 4x10G split cables are connected, the 40G port auto-channelizes to four 10G channels.
 - When 2x50G split cables are connected, the 100G port auto-channelizes to two 50G channels.
 - When 4x25G split cables are connected, the 100G port auto-channelizes to four 25G channels.
- **Support for consistent load balancing for ECMP groups (QFX10000)**—Starting with Junos OS Release 17.3R1 on QFX10000 switches, you can prevent the reordering of flows to active paths in an ECMP group when one or more paths fail. Only flows that are on inactive paths are redirected. This feature applies only to Layer 3 adjacencies learned through external BGP connections. It overrides the default behavior of disrupting all existing, including active, TCP connections when an active path fails. Include the **consistent-hash** statement at the `[edit policy-options policy-statement policy-statement-name then load-balance]` hierarchy level. You must also configure a global per-packet load-balancing policy.

[See [Understanding Consistent Load Balancing Through Resilient Hashing on ECMP Groups](#).]

- **CL74 FEC support for 25-gigabit and 50-gigabit channel speeds (QFX5200 switches)**—Starting with Junos OS Release 17.3, you can disable or reen able clause 74 (CL74)—as well as CL91—forwarding error correction (FEC) support on QFX5200 switches. FEC CL91 is supported for the 100-gigabit port speed and FEC CL74 is supported for both 25-gigabit and 50-gigabit port speeds. FEC CL91 is enabled by default for the 100-gigabit port speed; when the ports are channelized either in 4x25-gigabit or 2x50-gigabit, FEC CL74 is enabled.

- To disable the FEC mode:

```
[edit]
set interfaces interface-name together-options fec none
```

- To reen able the FEC mode:

```
[edit]
delete interfaces interface-name gigether-options fec none
```

or

```
[edit]
set interfaces interface-name gigether-options fec (fec74|fec91)
```

- To check FEC status:

```
show interfaces interface-name
```

The output for the show command will list FEC statistics for a particular *interface-name*, including the FEC corrected errors count, the FEC uncorrected errors count, and the type of FEC that was disabled or enabled.

Layer 2 Features

- **Support to exclude IRB Interfaces from state calculations (QFX5100)**—Starting with Junos OS Release 17.3R1, you can exclude a trunk or access interface from the state calculations for an IRB interface for member VLANs. An IRB interface typically has multiple ports in a single VLAN. Excluding trunk and access interfaces from state calculations means that as soon as the port specifically assigned to the VLAN goes down, the IRB interface for the VLAN is marked as down. Include the **autostate-exclude** statement at the **[edit interfaces ether-options]** hierarchy level. This feature was previously introduced in Junos OS Release 14.1X53-D40.

[See [Excluding an IRB Interface from State Calculations.](#)]

- **Increases number of vmembers to 256k for integrated routing and bridging interfaces and aggregated Ethernet interfaces (QFX10000 switches)**—To calculate how many interfaces are required to support 4,000 VLANs, for example, divide the maximum number of vmembers (256,000) by the number of configured VLANs (4,000). In this case, 64 interfaces are required.

Management

- **Enhancements to BGP peer sensors for Junos Telemetry Interface (QFX5110, QFX5200, and QFX10000)**—Starting with Junos OS Release 17.3R1, telemetry data streamed through gRPC for BGP peers is reported separately for each routing instance. To export data for BGP peers, you must now include the following path in front of all supported paths:
/network-instances/network-instance/[name_'instance-name']/protocols/protocol/

Additionally, the following paths are also now supported:

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

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

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

- **Support for LSP events and properties sensor for Junos Telemetry Interface (QFX5110 and QFX5200)**—Starting with Junos OS Release 17.3R1, you can export statistics for LSP events and properties through the Junos Telemetry Interface. Only gRPC streaming for this sensor is supported. You can export statistics for ingress point-to-point LSPs, point-to-multipoint LSPs, bypass LSPs, and dynamically created LSPs. To export data through gRPC, use the `/mpls/lsp/` or `/mpls/signal-protocols/` set of OpenConfig subscription paths. Use the **telemetrySubscribe** RPC to specify telemetry parameters and provision the sensor. If your device is running a version of Junos OS with an upgraded FreeBSD kernel, you must download the Junos Network Agent software package, which provides the interfaces to manage gRPC subscriptions. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models. This sensor was previously supported only on QFX10000 switches, MX Series routers, and PTX Series routers.

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

- **Support for the Junos Telemetry Interface (QFX5110 switches)**—Starting with Junos OS Release 17.3R1, you can provision sensors through the Junos Telemetry Interface to export telemetry data for various network elements without involving polling. On QFX5110 switches, only gRPC streaming of statistics is supported. UDP streaming is not supported.

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](#).]

- **Support for the Junos Telemetry Interface (QFX5110)**—Starting with Junos OS Release 17.3R1, you can provision sensors through the Junos Telemetry Interface to export telemetry data for various network elements without involving polling on QFX5110 switches. Only gRPC streaming of statistics is supported on QFX5110 switches. UDP streaming is not supported.

The following sensors are supported:

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

To provision sensors to stream data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters for a specified list of OpenConfig commands paths. You must download the Junos Network Agent software package, which provides the interfaces to manage gRPC subscriptions. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module and YANG models.

Support for the Junos Telemetry Interface was introduced on QFX10000 and QFX5200 switches in Junos OS Release 17.2R1.

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

Multicast

- **Support for static multicast route leaking for VRF and virtual-router instances (QFX5100 switches)**—Starting with Junos OS Release 17.3R1, you can configure your switch to share IPv4 multicast routes among different virtual routing and forwarding (VRF) instances or different virtual-router instances. Only multicast static routes with a destination-prefix length of /32 are supported for multicast route leaking. Only Internet Group Management Protocol version 3 is supported. To configure multicast route leaking for VRF or virtual-router instances, include the **next-table routing-instance-name.inet.0** statement at the **[edit routing-instances routing-instance-name routing-options static route destination-prefix/32]** hierarchy level. For **routing-instance-name**, include the name of a VRF or virtual-router instance. This feature was initially introduced in Junos OS Release 14.X53-D40.

[See [Understanding Multicast Route Leaking for VRF and Virtual-Router Instances.](#)]

Multiprotocol Label Switching (MPLS)

- **Support for Layer 2 circuit on aggregate interfaces (QFX10000 switches)**—Starting in Junos OS release 17.3R1, you can configure a Layer 2 circuit on aggregate interfaces. You can apply input and output VLAN tags for pop, swap, and push label operations on the VLAN-CCC interface. VLAN tags are applied when traffic is sent to and from the Layer 2 circuit interface. These operations are performed only on the outer TAG. The pop VLAN tag removes the VLAN tag from the top of the VLAN tag stack. The push VLAN tag adds a new outer VLAN tag, and the swap VLAN tag replaces the existing outer VLAN tag with the new VLAN tag. This feature provides interoperability between Layer 2 services with a distinct VLAN at the local or remote end, or for instances where the Layer 2 service comes with a certain VLAN, but the remote peer has a different VLAN or no VLAN.

[See [CCC Overview](#) .]

- **VRF support in IRB interfaces in a Layer 3 VPN (QFX5100 and QFX5100 Virtual Chassis)**—Starting in Junos Release 17.3R1, you can configure IRB interfaces under virtual routing and forwarding (VRF) in a VPN Layer 3 network. IRB interfaces enable a switch to recognize which packets are being sent to local addresses so that they are bridged whenever possible and are routed only when needed. This same functionality applies, when IRB interfaces are part of routing instances or VRF. Virtual routing instances allows you to divide the switch into multiple independent virtual routers, each with its own routing table. This increases functionality by allowing network paths to be segmented without using multiple devices. Because traffic is automatically segregated, VRF also increases network security and can eliminate the need for encryption and authentication. Internet service providers often take advantage of VRF to create separate VPNs for their customers.

[See [Understanding Virtual Routing and Forwarding Tables](#) .]

Network Management and Monitoring

- **Support for Static link protection on Aggregated interfaces (QFX5100 switches)**—Starting in Junos OS release 17.3R1, you can enable link protection on a specified static Label-Switched Paths (LSP). You can designate a primary and backup physical link to support link protection. Egress traffic passes only through the designated primary link. This includes transit traffic and locally generated traffic on the router. When the primary link fails, traffic is routed through the backup link.

Operation, Administration, and Maintenance

- **Junos daemons to natively emit JSON output (QFX Series)**—Starting with Junos OS Release 17.3R1, the operational state emitted by the daemons is supported in JSON format as well as XML format. To configure JSON format, specify the following CLI command: **set system export-format state-data json compact**. To specify JSON format for specific command output, include **display json** in specific CLI commands.
- **Junos OpenConfig to support operational models for VLANs (QFX Series)**—Starting with Junos OS Release 17.3R1, support has been added for an OpenConfig YANG model for VLANs via the addition of **openconfig-vlan.yang**, revision 1.0.2. This provides a unified view for the network agent to retrieve operational state from JUNOS daemons for VLANs.

Port Security

- **MAC-limiting support (QFX10000 switches)**—Starting in Junos OS Release 17.3R1, you can configure MAC limiting on QFX10000 Series switches. MAC limiting enhances port security by limiting the number of MAC addresses that can be learned within a VLAN. Limiting the number of MAC addresses protects the switch from flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). Flooding occurs when the number of new MAC addresses that are learned causes the Ethernet switching table to overflow, and previously learned MAC addresses are flushed from the table. The switch then reverts to flooding the previously-learned MAC addresses, which can impact performance and introduce security vulnerabilities.

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

[See [Understanding MAC Limiting and MAC Move Limiting for Port Security](#).]

- **IP source guard (QFX5100, QFX5110, QFX5200)**—Starting with Junos OS Release 17.3R1, you can configure the IP source guard access port security feature to mitigate the effects of source IP address spoofing and source MAC address spoofing. If IP source guard determines that a host connected to an access interface has sent a packet with an invalid source IP address or source MAC address in the packet header, it discards the packet.

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

Routing Protocols Policy and Firewall Filters

- **Flexible Ethernet Support (QFX10000 switches)**—Starting in Junos OS release 17.3R1, you can configure `inet`, `inet6`, or `vlan-circuit` cross-connect (CCC) connections on a physical or aggregate ethernet interface. This allows you to set different forwarding rules for tagged and untagged traffic on the same interface. For example, you can forward tagged packets over the `l2circuit` and route untagged traffic normally in the native vlan mode.

All logical devices that are under the flexible vlan tagging are identified by their `vlan-id` configuration. For untagged traffic, the association to the corresponding logical device is derived using the native vlan id configuration on the physical device. For traffic without a vlan tag, the default vlan id (native vlan id) is used to derive the layer2 domain.

Routing Protocols

- **Support for BGP Large Communities (QFX Series)**—Starting with Junos OS 17.3R1, BGP community is enhanced to support BGP large community that uses 12-byte encoding where the most significant 4-bytes encode autonomous system number or global administrator and the remaining two 4-bytes encode operator defined local values. Currently, BGP normal community (4-byte) and BGP extended community (6-byte) provide limited support for BGP community attributes after the introduction of 4-byte autonomous system number. Configure the large BGP community attributes under `[edit policy-options community community-name members]` hierarchy level and under `[edit routing-options static route route community]` hierarchy level with keyword **large** followed by three 4-byte unsigned integers separated by colons. The attributes are represented as `large:autonomous system number:local value 1:local value2`.
- **Support for segment routing for IS-IS (QFX5110 and QFX5200)**—Starting with Junos OS Release 17.3R1, you can advertise MPLS labels through IS-IS to support segment routing. IS-IS advertises a set of segments, which enables an ingress device to steer a packet through a specific set of nodes and links in the network without relying on the intermediate nodes in the network to determine the path to take. Two types of segments are supported: node and adjacency. A node segment represents a shortest-path link to a node. An adjacency segment represents a specific adjacency to a node. To enable segment routing, include the `source-packet-routing` statement at the `[edit protocols isis]` hierarchy level. By default, segment routing is enabled on all IS-IS levels. To disable advertising of the adjacency segment for a specified interface, include the `no-advertise-adjacency-segment` statement. You can also specify an interval for maintaining adjacency segments by including the `adjacency-segment hold-time milliseconds` statement.

To enable node segments, include the `node-segment` statement at the `[edit protocols isis source-packet-routing]` hierarchy level. You have two options for advertising a range of indices for IPv4 or IPv6 addresses. Use the `index-range` statement to specify a dynamic label range managed by MPLS. To specify a specific block of indices, also known as a segment routing global block, include the **start-label index-range** statements at the `[edit protocols isis source-packet-routing srgb]` hierarchy level. This configuration enables MPLS to reserve the specified label range. Segment routing in IS-IS also supports provisioning prefix segment indices (SIDs) and anycast SIDs for both IPv4 and IPv6 prefixes. These SIDs

are provisioned through a routing policy for each prefix. Include the **prefix-segment index number** statement at the **[edit policy options policy-statement *policy-name* then]** hierarchy level. You can also enable IPG shortcuts for prefix segment routes. Include the shortcuts statement at the **[edit protocols isis traffic-engineering family (inet-mpls | inet6-mpls)]** hierarchy level.

This feature was introduced on QFX5100 and QFX10000 switches in Junos OS Release 17.2R1.

[See [Understanding Source Packet Routing](#).]

- **BGP precision-timer support for reducing BGP hold-time (QFX5100, QFX5100 Virtual Chassis, QFX5110, QFX5200, QFX10000)**—Starting in Junos OS Release 17.3R1, you can use BGP precision timers to enable BGP sessions to send frequent keepalive messages with hold times as short as 10 seconds. The hold time is the maximum time allowed to elapse between successive keepalive messages that BGP receives from a peer. The default hold time is 90 seconds; the default frequency for keepalive messages is 30 seconds. More frequent keepalive messages and shorter hold times might be desirable in large-scale deployments with many active sessions. When you set a **hold-time** value to less than 20 seconds, we recommend that you also configure the BGP **precision-timers** statement, so that if scheduler slip messages occur, the routing device continues to send keepalive messages. When the **precision-timers** statement is included, keepalive messages are generated in a dedicated kernel thread, thus helping to prevent BGP session flaps.

[See [precision-timers](#).]

- **Support for 128 equal-cost paths for BGP multipath (QFX10000)**—Starting with Junos OS Release 17.3R1, you can configure a maximum of 128 equal-cost paths for external BGP peers. Previously, the maximum number supported was 64. For MPLS routes, the maximum number of equal-cost paths you can configure remains unchanged at 64. To specify 128 equal-cost paths for external BGP peers, include the **maximum-ecmp 128** statement at the **[edit chassis]** hierarchy level. You must also configure a routing policy that exports routes from the routing table into BGP. Define a routing policy by including the **policy-statement *policy-name*** set of statements at the **[edit policy-options]** hierarchy level. Apply the policy to routes exported to the forwarding table by including the **export *policy-name*** statement at the **[edit routing-options forwarding-table]** hierarchy level.

[See [maximum-ecmp](#).]

NOTE: This feature is released but not supported in Junos OS Release 17.3R1.

- **Support for segment routing for OSPF (QFX5110 and QFX5200)**—Starting with Junos OS Release 17.3R1, you can advertise MPLS labels through OSPF to support segment routing. Only IPv4 is supported. OSPFv3 is not supported. OSPF advertises a set of segments, which enables an ingress device to steer a packet through a specific set of nodes and links in the network without relying on the intermediate nodes in the network to determine the path to take. Two types of segments are supported: node and adjacency. A node segment represents a shortest-path link to a node. An adjacency segment represents a specific adjacency to a node. To enable segment routing, include the **source-packet-routing** statement at the **[edit protocols ospf]** hierarchy level. By default, segment routing is enabled for all OSPF areas.

To disable for a specific area, include the **no-source-packet-routing** statement at the **[edit protocols ospf area *area-id*]** hierarchy level. To enable node segments, include the **node-segment** statement. You can specify a range for IPv4 addresses to advertise, which MPLS manages dynamically. To disable advertising of the adjacency segment for a specified interface, include the **no-advertise-adjacency-segment** statement.

This feature was introduced on QFX5100 and QFX10000 switches in Junos OS Release 17.2R1.

[See [source-packet-routing](#).]

- **Support for alternate loop-free routes for IS-IS and OSPF (QFX10000)**—Starting in Junos OS Release 17.3R1, this feature adds fast reroute capability for IS-IS and OSPF. Junos OS precomputes loop-free backup routes for all IS-IS or OSPF routes. These backup routes are preinstalled in the Packet Forwarding Engine, which performs a local repair and implements the backup path when the link for a primary next hop for a particular route is no longer available. A loop-free path is one that does not traverse the router to reach a given destination. That is, a neighbor that already forwards traffic to the router is not used as a backup route to that destination.

You can enable support for alternate loop-free routes on any IS-IS or OSPF interface. To provide this support automatically for LDP label-switched paths (LSPs), you must also enable LDP on any interface for which you enabled support for loop-free alternate routes. In addition, you can extend backup coverage to include RSVP LSP paths.

Junos OS provides two mechanisms to enable fast reroute for IS-IS or OSPF using alternate loop-free routes: link protection and node-link protection. When you enable link protection or node-link protection on an IS-IS or OSPF interface, the software creates an alternate path to the primary next hop for all destination routes that traverse a protected interface. Link protection offers per-link traffic protection. It supports fast rerouting of user traffic over one mission-critical link. Node-link protection establishes an alternate path through a different router altogether.

[See [Loop-Free Alternate Routes for OSPF Overview](#), [Example: Configuring Link and Node Protection for IS-IS Routes](#).]

- **Support for alternate loop-free routes for IS-IS and OSPF (QFX5110 and QFX5200)**—Starting in Junos OS Release 17.3R1, this feature adds fast reroute capability for IS-IS and OSPF. Junos OS precomputes loop-free backup routes for all IS-IS or OSPF routes. These backup routes are preinstalled in the Packet Forwarding Engine, which performs a local repair and implements the backup path when the link for a primary next hop for a particular route is no longer available. A loop-free path is one that does not traverse the router to reach a given destination. That is, a neighbor that already forwards traffic to the router is not used as a backup route to that destination.

You can enable support for alternate loop-free routes on any IS-IS or OSPF interface. To provide this support automatically for LDP label-switched paths (LSPs), you must also enable LDP on any interface for which you enabled support for loop-free alternate routes. In addition, you can extend backup coverage to include RSVP LSP paths.

Junos OS provides two mechanisms to enable fast reroute for IS-IS or OSPF using alternate loop-free routes: link protection and node-link protection. When you enable link protection or node-link protection

on an IS-IS or OSPF interface, the software creates an alternate path to the primary next hop for all destination routes that traverse a protected interface. Link protection offers per-link traffic protection. It supports fast rerouting of user traffic over one mission-critical link. Node-link protection establishes an alternate path through a different router altogether.

[See [Loop-Free Alternate Routes for OSPF Overview](#), [Example: Configuring Link and Node Protection for IS-IS Routes](#).]

- **Support for BGP link-state distribution extensions for segment routing (QFX5110 and QFX5200)**—Starting in Junos OS Release 17.3R1, BGP link-state distribution extensions export segment-routing topology information to software-defined networking controllers. Although controllers can obtain the topology information by either being a part of an interior gateway protocol (IGP) domain or through BGP link-state distribution, the latter provides a more scalable mechanism for exporting this information. BGP link-state distribution is supported on inter-domain networks. This feature is useful in networks that are moving to segment routing at the transport layer but also have RSVP deployed. Include the **ipv4-prefix** statement at the **[edit policy-options policy-statement policy-name term term-name from traffic-engineering]** hierarchy level. This feature was introduced in Junos OS Release 17.2R1 on MX Series and PTX Series routers and on QFX5100 and QFX10000 switches.

[See [Link-State Distribution Using BGP Overview](#).]

Virtual Chassis

- **Virtual Chassis and Virtual Chassis Fabric (VCF) support (QFX5110)**—Starting with Junos OS Release 17.3R1, QFX5110 switches can be interconnected into a Virtual Chassis or VCF and operate as one logical device managed as a single chassis, as follows:
 - QFX5110 Virtual Chassis: Up to 10 members, all QFX5110 switches or in combination with QFX5100 switches. We recommend using QFX5110 switches in the master and backup Routing Engine roles, and QFX5100 switches only in the linecard role.
 - QFX5110 VCF: Up to 20 members, all QFX5110 switches or in combination with QFX5100 switches. Spine members must be QFX5110-32Q switches.
 - A QFX5110 Virtual Chassis or VCF can contain QFX5110-32Q, QFX5110-48S, QFX5100-24Q, QFX5100-48S, and QFX5100-98S switches. The same software image runs on QFX5110 or QFX5100 switches in a Virtual Chassis or VCF, and you do not need to configure the switches into mixed mode.



CAUTION: Any QFX5100 switches running a “-qfx-5-” Junos OS software image *must* first be upgraded to a “-qfx-5e-” image (using the USB method) to successfully join a mixed QFX5110 Virtual Chassis or VCF.

- Any (non-channelized) 100-Gbps or 40-Gbps QSFP28 ports, 40-Gbps QSFP+ ports, or 10-Gbps SFP+ ports can be Virtual Chassis ports (VCPs).

[See [Understanding QFX Series Virtual Chassis](#) and [Understanding QFX Virtual Chassis Fabric Components](#).]

SEE ALSO

Changes in Behavior and Syntax	 179
Known Behavior	 181
Known Issues	 183
Resolved Issues	 187
Documentation Updates	 189
Migration, Upgrade, and Downgrade Instructions	 190
Product Compatibility	 203

Changes in Behavior and Syntax

IN THIS SECTION

- [General Routing](#) | [180](#)
- [Management](#) | [180](#)
- [Network Management and Monitoring](#) | [181](#)
- [VLAN Infrastructure](#) | [181](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 17.3R1 for the QFX Series.

General Routing

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

[See [Enabling BFD on Qualified Next Hops in Static Routes for Route Selection](#).]

Management

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

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

Network Management and Monitoring

- **Enhancement to about-to-expire logic for license expiry syslog messages (QFX Series)**—As of Junos OS Release 17.3R1, the logic for multiple capacity type licenses and when their expiry raises alarms was changed. Before, the behavior had alarms and syslog messages for expiring licenses raised based on the highest validity, which would mislead users in the case of a license expiring earlier than the highest validity license. The new behavior has the about-to-expire logic based on the first expiring license.

VLAN Infrastructure

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

SEE ALSO

[New and Changed Features | 164](#)

[Known Behavior | 181](#)

[Known Issues | 183](#)

[Resolved Issues | 187](#)

[Documentation Updates | 189](#)

[Migration, Upgrade, and Downgrade Instructions | 190](#)

[Product Compatibility | 203](#)

Known Behavior

IN THIS SECTION

- [EVPNs | 182](#)
- [High Availability \(HA\) and Resiliency | 182](#)
- [Infrastructure | 182](#)
- [Interfaces and Chassis | 182](#)
- [Layer 2 Features | 182](#)
- [Routing Protocols | 183](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 17.3R1 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.

EVPNs

- EVPN/VXLAN implementations support up to 100 EVPN VLAN-based routing instances. Above 100 instances, MAC learning may behave incorrectly. [PR1287644](#)
- On QFX10000 switches implementing EVPN/VXLAN, if the routing engine is repeatedly restarted on redundant gateways, then inter-vrf traffic will be dropped without notification. [PR1289091](#)

High Availability (HA) and Resiliency

- During a nonstop software upgrade (NSSU) on an QFX5100 Virtual Chassis, a traffic loop or loss might occur if the Junos OS software version that you are upgrading and the Junos OS software version that you are upgrading to use different internal message formats. [PR1123764](#)
- On an EX4300 or a QFX5100 Virtual Chassis, when you perform an NSSU, there might be more than five seconds of traffic loss for multicast traffic. [PR1125155](#)

Infrastructure

- Multiple instances of the **DAEMON-3-JTASK_SCHED_SLIP** system message may be logged when over 50,000 MACs are configured and the device attempts to establish OSPF neighbors. This has no functional impact. [PR1274706](#)

Interfaces and Chassis

- If port speed is changed in from 25G to 100G or there are repeated changes in port speed settings, then the link may remain down. This is a Broadcom SDK limitation and has been addressed in Broadcom SDK versions 6.5.8 and above. [PR1250891](#)

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](#)
- When the replication tree used for flooding is reconverging, because some of the leaves have been deleted or added, there is expected to be some transient traffic loss even in leaves that have not changed. This affects only flooding and BUM traffic, not known unicast traffic. [PR1274950](#)

Routing Protocols

- An adjacency segment identifier will not be created for IPv6-only configured interfaces. If the adjacency uses IP alone or IP+IPv6, then an IPv4 adjacency segment identifier or IPv6 adjacency segment identifier will be created. If the adjacency only uses IPv6, then no adjacency segment identifier will be created.
[PR1290515](#)

SEE ALSO

New and Changed Features 164
Changes in Behavior and Syntax 179
Known Issues 183
Resolved Issues 187
Documentation Updates 189
Migration, Upgrade, and Downgrade Instructions 190
Product Compatibility 203

Known Issues

IN THIS SECTION

- [EVPNs | 184](#)
- [Interfaces and Chassis | 184](#)
- [IPsec | 186](#)
- [Multiprotocol Label Switching \(MPLS\) | 186](#)
- [Routing Protocols | 186](#)
- [System Management | 186](#)
- [VLAN Infrastructure | 186](#)

This section lists the known issues in hardware and software for the QFX Series switches in Junos OS Release 17.3R1.

EVPNs

- On QFX10000 switches, sub-interfaces from the same physical port do not work if configured under the same VLAN or routing-instance. An attempt to commit such a configuration will fail for Layer 2 configurations but not for EVPN/VXLAN. For EVPN/VXLAN configurations, there may be circumstances where it would be necessary to configure a sub-interface from the same physical port to support VLAN bundling. [PR1278761](#)
- Using EVPN/VXLAN, VLAN-ID *none* should be used for VLANs or routing instances using an IRB as the routing interface. [PR1287565](#)
- On QFX10000 switches, there will be minor traffic loss when more than 4000 VXLAN network identifiers (VNIs) are configured along with an EVPN/VXLAN overlay and an MPLS underlay. [PR1289666](#)
- In some scenarios, EVPN withdraw message is not sent after cleaning up the ARP/NDP/MAC table. [PR1293176](#)
- If the network includes a vlan-tagged inet interface, then EVPN layer 3 traffic will be corrupted and dropped. Customers must either change any vlan-tagged inet interface in their network to untagged or avoid using Junos OS release 17.3R1. [PR1295491](#)
- On a QFX10000 switch running Junos OS Release 17.3R1, the **df-election-type preference** statements in the **[show interfaces esi]** hierarchy level appear and can be configured and committed. However, QFX10000 switches do not actually support the use of these statements. [PR1300093](#)

Interfaces and Chassis

- On a QFX5100 Virtual Chassis, the MAC address is not learned on an ae- interface configured as a VXLAN Layer 2 port and with the interface mode configured as access. The issue is observed only with ae- interfaces that span multiple Virtual Chassis members and when the member node is rebooted or power cycled. [PR1112790](#)
- In a data center interconnect (DCI) scenario, when two QFX5100-24Qs in different data centers are interconnected using a 40G link and when DWDM is used in the connection especially with ADVA and single mode fiber (SMF) on one side and multi mode fiber (MMF) on the other, the 40G connection between the two QFX5100-24Qs may not be stable. Sometimes the link will come up and sometimes not. Frame errors might be seen constantly. [PR1178799](#)
- On a QFX5110-48S switch, a Gigabit Ethernet interface goes down and comes back up once on a peer as part of a reboot. [PR1237572](#)
- On a QFX5110-32C switch, if a splitter cable is connected to a Spirent 10G CV/MX card, ports won't come up due to varied pre-empt settings for the splitter and DAC cables. There is a hardware limitation where we have no way in EEPROM to differentiate between splitter and DAC cable to apply different settings. Use a 40G Spirent card with internal channelization on the Spirent side and manual channelization on the QFX5110-32C side as a workaround. [PR1280593](#)

- In an MC-LAG scenario with two QFX10000 switches configured in active-active mode, when a multicast packet is received by one of the MC-LAG member links, the packet will be forwarded on the ICL, and then it may be forwarded on the other mc-ae interface. So the multicast data packets are looping in MC-LAG. The packets get sent back to the source and dropped there. This path (ICL to MC-AE) should be blocked when both mc-ae interfaces are up, and should not be forwarded to the MC-AE interface. As a workaround, apply ICL filter to block multicast packets. [PR1281646](#)
- On QFX5100 switches, static LAG link protection switch-over / revert is not working consistently. [PR1286471](#)
- On QFX10000 switches, flexible VLAN-tagging interfaces are not supported with multiple virtual switching instances. [PR1287656](#)
- Proxy-ARP and ARP suppression is not supported on QFX10000 switches. [PR1293707](#)
- The QFX10000-60S switch experiences a heap memory leak. The following message is logged in /var/log: **dcpcfe: Heap memory utilization crossed 90 Percent, reached to 91 percent.** [PR1294208](#)
- Whenever an MC-AE interface is deactivated or activated on an MC-LAG node, once the MC-AE interfaces are back up, the system clears neighbor discovery entries on the ICL which triggers a neighbor discovery solicit and thereby neighbor discovery entries are learned on the MC-AE interface. Workaround is to clear neighbor discovery entries on the ICL whenever MC-AE interfaces have been deactivated or activated on MC-LAG nodes. [PR1294958](#)
- When link-protection with the backup port state 'down' and LACP are both configured, sometimes the primary port state becomes down without a trigger event and the backup port comes up and begins handling traffic. [PR1297596](#)
- When link-protection with the backup port state 'down' and LACP are configured, if backup-state 'down' is removed from the configuration, what should happen is that both ports will be up and the primary should pass all egress traffic. In some instances, traffic may instead pass through the backup rather than the primary port. [PR1297597](#)

- On QFX5100, QFX5110, and QFX5200 switches, IGMP snooping entries may not be synced to the MC-LAG peer sometimes. After configuring IGMP snooping, check the output of "show iccp". If MCSNOOPD is not shown as "Client Application", this problem will be observed. [PR1302620](#)

IPsec

- On some QFX-Series platforms including QFX5110, QFX5200 and QFX10k platforms, the OSPFv3 authentication using IPsec SA does not work, which might cause the OSPFv3 neighbors not to be established. [PR1301428](#)

Multiprotocol Label Switching (MPLS)

- MPLS egress traffic may fail when ingress Layer 3 and other MPLS application traffic is expected to transit via IRB with a Layer 2 interface in the core and MPLS encapsulation. [PR1279827](#)

Routing Protocols

- After clearing the IS-IS database, a label switched path (LSP) does not regenerate when the routing instance is purged. [PR1275573](#)
- On QFX5110 switches, an EVPN/VXLAN configuration using a custom-IRB MAC (same IP, same MAC profile) may not work. Using a virtual-gateway address is recommended. [PR1291406](#)

System Management

- On QFX10002 switches, the **request system snapshot** command does not work. [PR1048182](#)

VLAN Infrastructure

- When a VLAN uses an IRB interface as the routing interface, the vlan-id parameter must be set to "none" to ensure proper traffic routing. This issue is platform independent. [PR1287557](#)

SEE ALSO

[New and Changed Features | 164](#)

[Changes in Behavior and Syntax | 179](#)

[Known Behavior | 181](#)

[Resolved Issues | 187](#)

[Documentation Updates | 189](#)

[Migration, Upgrade, and Downgrade Instructions | 190](#)

[Product Compatibility | 203](#)

Resolved Issues

IN THIS SECTION

- [General Routing | 187](#)
- [Interfaces and Chassis | 187](#)
- [Layer 2 Features | 188](#)
- [Port Security | 188](#)
- [Routing Protocols | 188](#)
- [System Management | 188](#)
- [VXLAN | 188](#)

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.

General Routing

- VLAN association is not being updated in the Ethernet switching table when the device is configured in single supplicant mode. [PR1283880](#)
- Hostname synchronization from Junos VM instance to Linux Host in TVP Platforms (QFX). [PR1283710](#)

Interfaces and Chassis

- Interfaces randomly do not come up after a line card restart. [PR1262839](#)
- On QFX5100 switches, a 40G interface may keep flapping when a 5M DAC cable is inserted. [PR1273861](#)
- On QFX10000 switches, there may be an ot- link flap whenever there is an optics TCA alarm, however there is no loss of signal and no traffic loss observed. [PR1279351](#)
- FEC disabled by default on 100G-LR optics for QFX5200 switches. [PR1286389](#)

Layer 2 Features

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

Port Security

- On QFX10000 switches, MACsec sessions are not coming up on a Layer 3 sub-interface. [PR1282995](#)

Routing Protocols

- When static Link protection mode configured back up state as down, primary port is going to down state instead of secondary port while secondary is at up state. [PR1276156](#)
- UDP traffic with destination port 520 and 521 is discarded on QFX5110 switches after a Junos OS upgrade. [PR1287271](#)
- In a data center environment with EVPN/VXLAN and proxy MAC plus IP advertisement enabled on a Layer 3 gateway, the state for some MACs may be lost during MAC moves. [PR1291118](#)

System Management

- Multicast Listener Discovery (MLD) messages are seen continuously on QFX switches if the management ports are connected through a network. [PR1277618](#)
- Analytics json data format reporting incorrect value for 'rxbps' counter. [PR1285434](#)

VXLAN

- Two new CLI commands are added: **set forwarding-options vxlan-routing next-hop *number*** ; **set forwarding-options vxlan-routing interface-num *number***. These commands are applicable only for QFX5110 switches. [PR1259323](#)

SEE ALSO

New and Changed Features 164
Changes in Behavior and Syntax 179
Known Behavior 181
Known Issues 183
Documentation Updates 189

[Migration, Upgrade, and Downgrade Instructions | 190](#)

[Product Compatibility | 203](#)

Documentation Updates

IN THIS SECTION

- [Traffic Management User Guide for the QFX Series | 189](#)

This section lists the errata and changes in Junos OS Release 17.3R1 for the QFX Series switches documentation.

Traffic Management User Guide for the QFX Series

- **Consolidation of the Traffic Management User Guide for QFX Series and EX4600 Switches (QFX Series)**—Starting in Junos OS Release 17.3R1, the following three traffic management guides are consolidated into one user guide:
 - Traffic Management User Guide for QFX Series
 - Traffic Management User Guide for QFX 10000 Series
 - Traffic Management User Guide for EX4600 Switches

[See [Traffic Management User Guide for QFX Series and EX4600 Switches](#).]

SEE ALSO

[New and Changed Features | 164](#)

[Changes in Behavior and Syntax | 179](#)

[Known Behavior | 181](#)

[Known Issues | 183](#)

[Resolved Issues | 187](#)

[Migration, Upgrade, and Downgrade Instructions | 190](#)

[Product Compatibility | 203](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrading Software on QFX Series Switches | 190
- Installing the Software on QFX10002 Switches | 193
- 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 | 193
- Installing the Software on QFX10008 and QFX10016 Switches | 195
- Performing a Unified ISSU | 199
- Preparing the Switch for Software Installation | 200
- Upgrading the Software Using Unified ISSU | 200

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 **17.3** in the Release pull-down list to the right of the Software tab on the Download Software page.
4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 17.3 release.

An Alert box appears.

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

A login screen appears.

6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Download the software to a local host.
8. Copy the software to the device or to your internal software distribution site.
9. Install the new jinstall package on the device.

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

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

```
user@host> request system software add source/jinstall-qfx-5-17.3 -R3.n-domestic-signed.tgz
reboot
```

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 17.3 **jinstall** package, you can issue the **request system software rollback** command to return to the previously installed software.

Installing the Software on QFX10002 Switches

NOTE: If you are upgrading from a version of software that does not have the FreeBSD 10 kernel (15.1X53-D30, for example), you will need to upgrade from Junos OS Release 15.1X53-D30 to Junos OS Release 15.1X53-D32. After you have installed Junos OS Release 15.1X53-D32, you can upgrade to Junos OS Release 15.1X53-D60 or Junos OS Release 17.3R1.

NOTE: On the switch, use the **force-host** option to force-install the latest version of the Host OS. However, by default, if the Host OS version is different from the one that is already installed on the switch, the latest version is installed without using the **force-host** option.

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

For example:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-17.3R1.n-secure-signed.tgz
reboot
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> reboot** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-17.3R1.n-secure-signed.tgz reboot
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches

NOTE: Before you install the software, back up any critical files in `/var/home`. For more information regarding how to back up critical files, contact Customer Support at <https://www.juniper.net/support>.

The switch contains two Routing Engines, so you will need to install the software on each Routing Engine (re0 and re1).

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

To install the software on re0:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> re0** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

To install the software on re1:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> re1** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

Reboot both Routing Engines.

For example:

```
user@switch> request system reboot both-routing-engines
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Installing the Software on QFX10008 and QFX10016 Switches

Because the switch has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at <https://www.juniper.net/support>.



WARNING: If graceful Routing Engine switchover (GRES), nonstop bridging (NSB), or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you issue the CLI **delete chassis redundancy** command when prompted. If GRES is enabled, it will be removed with the **redundancy** command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the **[edit routing-options]** hierarchy level to disable it.

1. Log in to the master Routing Engine's console.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

2. From the command line, enter configuration mode:

```
user@switch> configure
```

3. Disable Routing Engine redundancy:

```
user@switch# delete chassis redundancy
```

4. Disable nonstop-bridging:

```
user@switch# delete protocols layer2-control nonstop-bridging
```

5. Save the configuration change on both Routing Engines:

```
user@switch# commit synchronize
```

6. Exit the CLI configuration mode:

```
user@switch# exit
```

After the switch has been prepared, you first install the new Junos OS release on the backup Routing Engine, while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the software version on the other Routing Engine.

7. Log in to the console port on the other Routing Engine (currently the backup).

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

8. Install the new software package using the **request system software add** command:

```
user@switch> request system software add validate
/var/tmp/jinstall-host-qfx-10-17.3R1.n-secure-signed.tgz
```

For more information about the **request system software add** command, see the [CLI Explorer](#).

9. Reboot the switch to start the new software using the **request system reboot** command:

```
user@switch> request system reboot
```

NOTE: You must reboot the switch to load the new installation of Junos OS on the switch.

To abort the installation, do not reboot your switch. Instead, finish the installation and then issue the **request system software delete <package-name>** command. This is your last chance to stop the installation.

All the software is loaded when you reboot the switch. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation is not sending traffic.

10. Log in and issue the **show version** command to verify the version of the software installed.

```
user@switch> show version
```

Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the master Routing Engine software.

11. Log in to the master Routing Engine console port.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

12. Transfer routing control to the backup Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the **request chassis routing-engine master** command, see the [CLI Explorer](#).

13. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

```
user@switch> show chassis routing-engine
```

```
Routing Engine status:
Slot 0:
  Current state           Backup
  Election priority       Master (default)
Routing Engine status:
Slot 1:
  Current state           Master
  Election priority       Backup (default)
```

14. Install the new software package using the **request system software add** command:

```
user@switch> request system software add validate
/var/tmp/jinstall-host-qfx-10-17.3R1.n-secure-signed.tgz
```

For more information about the **request system software add** command, see the [CLI Explorer](#).

15. Reboot the Routing Engine using the **request system reboot** command:

```
user@switch> request system reboot
```

NOTE: You must reboot to load the new installation of Junos OS on the switch.

To abort the installation, do not reboot your system. Instead, finish the installation and then issue the **request system software delete jinstall <package-name>** command. This is your last chance to stop the installation.

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation does not send traffic.

16. Log in and issue the **show version** command to verify the version of the software installed.

17. Transfer routing control back to the master Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the **request chassis routing-engine master** command, see the [CLI Explorer](#).

18. Verify that the master Routing Engine (slot 0) is indeed the master Routing Engine:

```
user@switch> show chassis routing-engine
```

```
Routing Engine status:
  Slot 0:
    Current state           Master
    Election priority       Master (default)
Routing Engine status:
  Slot 1:
    Current state           Backup
    Election priority       Backup (default)
```

Performing a Unified ISSU

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

NOTE: Unified ISSU is supported for upgrading to Junos OS Release 17.3R1 from 17.1R1 or later. Upgrading to 17.3R1 from releases prior to 17.1R1 is not supported. For example, upgrading from Junos OS Release 14.1X53 to 17.3R1 is not supported.

Perform the following tasks:

- [Preparing the Switch for Software Installation on page 200](#)
- [Upgrading the Software Using Unified ISSU on page 200](#)

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-5-17.3R1-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-qfx-5-13.2X51-D15.4-domestic ...
Install jinstall-qfx-5-13.2X51-D15.4-domestic completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
```

```

ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item          Status          Reason
  FPC 0         Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff

```

NOTE: A unified ISSU might stop, instead of abort, if the FPC is at the warm boot stage. Also, any links that go down and up will not be detected during a warm boot of the Packet Forwarding Engine (PFE).

NOTE: If the unified ISSU process stops, you can look at the log files to diagnose the problem. The log files are located at `/var/log/vjunos-log.tgz`.

5. Log in after the reboot of the switch completes. To verify that the software has been upgraded, enter the following command:

```
user@switch> show version
```

6. Ensure that the resilient dual-root partitions feature operates correctly, by copying the new Junos OS image into the alternate root partitions of all of the switches:

```
user@switch> request system snapshot slice alternate
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

SEE ALSO

[New and Changed Features | 164](#)

Changes in Behavior and Syntax 179
Known Behavior 181
Known Issues 183
Resolved Issues 187
Documentation Updates 189
Product Compatibility 203

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 203

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 164
Changes in Behavior and Syntax 179
Known Behavior 181
Known Issues 183
Resolved Issues 187

Documentation Updates | 189

Migration, Upgrade, and Downgrade Instructions | 190

Junos OS Release Notes for SRX Series

IN THIS SECTION

- New and Changed Features | 204
- Changes in Behavior and Syntax | 210
- Known Behavior | 216
- Known Issues | 222
- Resolved Issues | 225
- Documentation Updates | 227
- Migration, Upgrade, and Downgrade Instructions | 227
- Product Compatibility | 231

These release notes accompany Junos OS Release 17.3R1 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

- Flow and Processing | 205
- IDP | 206
- Interfaces and Chassis | 207
- Junos OS XML API and Scripting | 207
- Layer 2 Features | 207

- Management | 208
- Network Security | 208
- Software Installation and Upgrade | 208
- User Interface and Configuration | 209

This section describes the new features and enhancements to existing features in Junos OS Release 17.3R1 for the SRX Series devices.

Junos OS Release 17.3R1 supports the following Juniper Networks security platforms: vSRX, SRX300/320, SRX340/345, SRX550HM, SRX1500, SRX4100/4200, SRX5400, SRX5600, and SRX5800. Most security features in this release were previously delivered in Junos OS for SRX Series “X” releases from 12.1X44 through 15.1X49-D75. Security features delivered in Junos OS for SRX Series “X” releases after 15.1X49-D75 are not available in 17.3R1.

New features for security platforms in Junos OS Release 17.3R1 include:

Flow and Processing

- **ECMP reverse traffic support (SRX Series)**—Starting with Junos OS Release 17.3R1, you can enable ECMP support for reverse traffic. In this case, the SRX Series device uses a hash algorithm to determine the interface to use for reverse traffic in a flow. If you do not enable this feature, the SRX Series device selects a route in the ECMP set to the incoming interface for reverse traffic, which is the default behavior.
[See [Understanding ECMP Flow-Based Forwarding for Reverse Traffic on SRX Series Devices and vSRX](#)]
- **TCP out-of-state packet drop logging (SRX Series)**—Starting in Junos OS Release 17.3R1, SRX Series devices support logging of unsynchronized TCP out-of-state packets that are dropped by the flow module.

Within any packet-switched network, when demand exceeds available capacity, the packets are queued up to hold the excess packets until the queue fills, and then the packets are dropped. When TCP operates across such a network, it takes any corrective actions to maintain error-free end-to-end communications.

This feature enables packet recovery by logging the out-of-sync packets for error-free communication, and avoids database servers going out of sync.

TCP packet drop logging occurs when:

- TCP packets that trigger session creation are not synchronized.
- TCP three-way handshake in flow fails.

- TCP sequence check in flow fails.
- TCP SYN packets are received in TCP FIN state.

The unsynchronized TCP out-of-state packet drop log is a packet-based log, not a session-based log.

NOTE: TCP packets that are dropped by TCP-proxy and IDP are not logged.

[See [TCP Out-of-State Packet Drop Logging Overview](#).]

IDP

- **IPS signature package update (SRX Series and vSRX instances)**—Starting with Junos OS Release 17.3, when you upgrade from Junos OS Release 12.3X48 or 15.1X49 to Junos OS Release 17.3 or downgrade from Junos OS Release 17.3 to Junos OS Release 12.3X48 or 15.1X49, you must update the IPS signature package to avoid any IDP configuration commit failures. Update the IPS signature package by:
 - Downloading the IPS signature package
 - Installing the IPS signature package update when the download completes

NOTE: When you upgrade from Junos OS Release 15.1X49 to Junos OS Release 17.3, the following warning message is displayed:

```
WARNING: A full install of the security package is required after reboot.  
WARNING: Please perform a full update of the security package using  
WARNING: "request security idp security-package download full-update"  
WARNING: followed by  
WARNING: "request security idp security-package install"
```


[See [Downloading and Installing the IPS Signature Package from an Older Junos OS Release Version to Newer Junos OS Release Version.](#)]

Interfaces and Chassis

- **Promiscuous mode support [SRX5400, SRX5600, SRX5800]**—Promiscuous mode function is supported on the SRX5000 line MPC (SRX5K-MPC) on 1-Gigabit, 10-Gigabit, 40-Gigabit, and 100-Gigabit Ethernet interfaces on the MICs.

By default, an interface enables MAC filtering. You can configure promiscuous mode on the interface to disable MAC filtering. When you delete the promiscuous mode configuration, the interface will perform MAC filtering again. You can change the MAC address of the interface even when the interface is operating in promiscuous mode. When the interface is operating in normal mode again, the MAC filtering function on MPC uses the new MAC address to filter packets.

[See [Understanding Promiscuous Mode on Ethernet Interfaces.](#)]

Junos OS XML API and Scripting

- **Support for Python language for commit, event, op, and SNMP scripts (SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances)**—Starting in Junos OS Release 17.3R1, you can author commit, event, op, and SNMP scripts in Python on devices that include the Python extensions package in the software image. Creating automation scripts in Python enables you to take advantage of Python features and libraries as well as leverage Junos PyEZ APIs supported in Junos PyEZ Release 1.3.1 and earlier releases to perform operational and configuration tasks on devices running Junos OS. To enable execution of Python automation scripts, which must be owned by either root or a user in the Junos OS **super-user** login class, configure the **language python** statement at the **[edit system scripts]** hierarchy level, and configure the filename for the Python script under the hierarchy level appropriate to that script type. Supported Python versions include Python 2.7.

[See [Understanding Python Automation Scripts for Devices Running Junos OS.](#)]

Layer 2 Features

- **LACP support in Layer 2 transparent mode (SRX5400, SRX5600, and SRX5800)**—Starting with Junos OS Release 17.3, LACP is supported in Layer 2 transparent mode in addition to existing support in Layer 3 mode.

When the SRX Series device uses LACP to bundle the member links, it creates high-speed connections, also known as *fat pipe*, with peer systems. Bandwidth can be increased by adding member links. Increased bandwidth is especially important for redundant Ethernet (reth) and aggregated Ethernet (ae) interfaces. LACP also provides automatic determination, configuration, and monitoring member links.

LACP is compatible with other peers that run the 802.3ad LACP protocol. It automatically binds member links without manually configuring the LAG, thereby avoiding errors.

NOTE: Tentative sessions are created for all interfaces in a particular VLAN. If there is plenty of one-way traffic, numerous tentative sessions are created. When sessions reach the maximum limit, vector fails and packet loss might be seen.

Management

- **Support for adding non-native YANG modules to the Junos OS schema (SRX345, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances)**—Starting in Junos OS Release 17.3R1, you can load custom YANG models on devices running Junos OS to add data models that are not natively supported by Junos OS but can be supported by translation. Doing this enables you to extend the configuration hierarchies and operational commands with data models that are customized for your operations. The ability to add data models to a device is also beneficial when you want to create device-agnostic and vendor-neutral data models that enable the same configuration or RPC to be used on different devices from one or more vendors. You can load custom YANG modules by using the **request system yang add** operational command.

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

Network Security

- **Maximum number of security policies increased (SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 17.3R1, the maximum number of security policies for SRX5400, SRX5600, and SRX5800 devices has increased from 80,000 to 100,000.

[See [Best Practices for Defining Policies on SRX Series Devices.](#)]

Software Installation and Upgrade

- **Support for FreeBSD version 10 for Junos OS (SRX5800, SRX5600, SRX5400)**—Starting with Junos OS Release 17.3R1, on the SRX5000 line of devices, FreeBSD version 10 is the underlying operating system for Junos OS. Junos OS with upgraded FreeBSD is based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. The newer FreeBSD kernel base provides Junos OS with sophisticated processing, efficiency, and security.

NOTE: On SRX5000 line of devices, use **no-validate** flag at the **request system software add <filename> no-validate** command to upgrade or downgrade between Junos OS Release 17.3 and the previous releases.

NOTE: Along with the upgraded FreeBSD, the System Snapshot feature has been enhanced on the SRX5000 line of devices. For more details, see *Understanding Junos OS with Upgraded FreeBSD Snapshots* topic in [Understanding Junos OS with Upgraded FreeBSD for SRX5400, SRX5600, and SRX5800 Devices](#)

[See [Understanding Junos OS with Upgraded FreeBSD](#)]

User Interface and Configuration

- **Support for configuring the ephemeral database using the NETCONF and Junos XML protocols (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances)**—Starting in Junos OS Release 17.3, NETCONF and Junos XML protocol client applications can configure the ephemeral configuration database, which is an alternate configuration database that enables multiple clients to simultaneously load and commit configuration changes on a device running Junos OS and with significantly greater throughput than when committing data to the candidate configuration database. Junos OS provides a default instance and up to eight user-defined instances of the ephemeral configuration database. The device's active configuration is a merged view of the committed configuration database and the configuration data in all instances of the ephemeral configuration database. Ephemeral configuration data is volatile and is deleted upon rebooting the device.

[See [Understanding the Ephemeral Configuration Database](#).]

SEE ALSO

[Changes in Behavior and Syntax](#) | 210

[Known Behavior](#) | 216

[Known Issues](#) | 222

[Resolved Issues | 225](#)[Documentation Updates | 227](#)[Migration, Upgrade, and Downgrade Instructions | 227](#)[Product Compatibility | 231](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [ALGs | 211](#)
- [Access and User Management | 211](#)
- [Application Security | 211](#)
- [Authentication, Authorization and Accounting \(AAA\) | 211](#)
- [Chassis Cluster | 211](#)
- [CLI | 212](#)
- [Dynamic Host Configuration Protocol \(DHCP\) | 212](#)
- [Flow-based and Packet-based Processing | 213](#)
- [General Packet Radio Service \(GPRS\) | 213](#)
- [IDP | 214](#)
- [J-Web | 214](#)
- [Layer 2 Features | 214](#)
- [NAT | 214](#)
- [Network Management and Monitoring | 215](#)
- [System Logs | 215](#)
- [Unified Threat Management \(UTM\) | 215](#)
- [VLAN Infrastructure | 216](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 17.3R1.

ALGs

- Starting with Junos OS Release 17.3R1, the custom application UUID with leading zeros does not match all TCP traffic and referenced policies, which will enter MS-RPC ALG check. This new application does not allow the nil UUID. In earlier releases, on all SRX Series devices, the custom application universal unique identifier (UUID) of Microsoft remote procedure call (MS-RPC) with leading zeros and the nil UUID (00000000-0000-0000-0000-000000000000) might match all TCP traffic and referenced policies allowing all TCP traffic instead of entering MS-RPC ALG check.

Access and User Management

- Starting from Junos OS Release 17.3R1, for configuring the root login through SSH to control user access, the default option is **system services ssh root-login deny-password**. In previous releases, the default option was **system services ssh root-login allow**.

Now, to allow users to log in to the device as root through SSH, you must configure the root login explicitly using the **set system services ssh root-login allow** option.

Application Security

- **Application-level distributed denial of service**— On SRX Series devices, application-level distributed denial of service (AppDDoS), which is used to identify malicious bot clients and to drop or deny traffic if requests exceed configured thresholds, is deprecated. This feature was deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Starting with Junos OS Release 17.3, AppDDoS is removed as per the Juniper Networks deprecation process. If you are using any previous versions of Junos OS Release and want to upgrade to Junos OS Release 17.3, you must remove all the configurations related to AppDDoS to avoid any disruption during the upgrade.

Authentication, Authorization and Accounting (AAA)

- The **options no-hostname** is added to the dhcp-client configuration. You set the no-hostname if you do not want the DHCP client to send the hostname with the packets (DHCP option code 12).

Chassis Cluster

- **Chassis cluster initial hold timer**—The initial hold timer is extended from 30 seconds to 120 seconds in chassis clusters on SRX340 and SRX345 devices.
- **Chassis cluster ineligible timer**—The ineligible timer is 5 minutes when MACsec on the chassis cluster

control port is enabled on SRX340 and SRX345 devices.

- **802.1x-protocol-daemon**—The 802.1x protocol process (daemon) does not support restart on SRX340 and SRX345 devices.
- There is a change in the method for calculating the memory utilization by a Routing Engine. The inactive memory is now considered free and is no longer included in the calculation of memory utilization. That is, the value for used memory shown in the output of the **show chassis routing-engine** command decreases and results in more memory to be available for other processes.

CLI

- The **modem1** option has been added to the **show wireless-wan adapter <adapter name> modem** command. The **modem1** option displays details of the integrated modems on the CBA850 3G/4G/LTE Wireless WAN Bridge.

Dynamic Host Configuration Protocol (DHCP)

- The legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI will be supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

To ensure uninterrupted service to existing user implementation of DHCP relay service, the following configuration items are identified as missing (edit and interface hierarchies) between the old DHCPD and the new JDHCPD configurations:

```
set forwarding-options helpers bootp description
set forwarding-options helpers bootp client-response-ttl
set forwarding-options helpers bootp maximum-hop-count
set forwarding-options helpers bootp minimum-wait-time
set forwarding-options helpers bootp vpn
set forwarding-options helpers bootp relay-agent-option
set forwarding-options helpers bootp dhcp-option82
```

and the interface hierarchy:

```
set forwarding-options helpers bootp interface interface-name description
set forwarding-options helpers bootp interface interface-name client-response-ttl
set forwarding-options helpers bootp interface interface-name maximum-hop-count
set forwarding-options helpers bootp interface interface-name minimum-wait-time
```

```
set forwarding-options helpers bootp interface interface-name vpn
set forwarding-options helpers bootp interface interface-name relay-agent-option
set forwarding-options helpers bootp interface interface-name dhcp-option82
```

- **Change in Dynamic Host Configuration Protocol (DHCP) configuration**—Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option **dhcp-client** at **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy is changed to **dhcp** to align with other Junos OS platforms. There is no change in the functionality.

[See [Example: Configuring the Device as a DHCP Client](#) and [dhcp-client](#).]

Flow-based and Packet-based Processing

- **Change to show security flow status command output (SRX300, SRX320, SRX340, SRX345, and SRX550M)**—Starting in Junos OS Release 17.3, the output field **ISO forwarding mode** for the **show security flow status** command displays the following warning message when the ISO forwarding mode is changed to packet-based: **reboot needed to change to packet-based**, and the following warning message displays when the packet-based ISO forwarding mode is deleted: **reboot needed to change to drop**.
- **Source address for SRX5400, SRX5600, and SRX5800 devices and vSRX2.0 instances**—Management traffic can originate from a specific source address for Domain Name System (DNS) names.

Consider the following when you configure the source address for DNS:

- Only one source address can be configured as the source address for each DNS server name.
- IPv6 source addresses are supported for IPv6 DNS servers, and only IPv4 addresses are supported for IPv4 DNS servers. You cannot configure an IPv4 address for an IPv6 DNS server or an IPv6 address for an IPv4 DNS server.

To have all management traffic originate from a specific source address, configure the system name server and the source address. For example:

```
user@host# set system name-server 5.0.0.1 source-address 4.0.0.3
```

General Packet Radio Service (GPRS)

- Prior to Junos OS Release 17.3R1, multi-chunk inspection was disabled by default and you could enable or disable by performing the following configurations:
 - **set security gprs sctp multichunk-inspection enable**
 - **set security gprs sctp multichunk-inspection disable**

Starting from Junos OS Release 17.3R1, multi-chunk inspection is enabled by default and you can disable by configuring the **set security gprs sctp multichunk-inspection disable** command.

- The Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN) of the GTPv1 or GTPv2 nodes cannot communicate with the GTPv0 node. If a device sends a GTPv1 or GTPv2 message to update the tunnels created by GTPv0, these messages are dropped and the GTPv0 tunnel will not be updated.

IDP

- For all SRX Series devices, configuration of patterns in standard PCRE format is supported in the custom attacks.

J-Web

- J-Web supports only the new CLI configurations. For more information, see <https://kb.juniper.net/InfoCenter/index?page=content&id=TSB16991>

Layer 2 Features

- **LLDP and LLDP-MED for SRX300, SRX320, SRX340, SRX345, SRX550M and SRX1500 devices**—Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discovery (MFD) are enabled on SRX300, SRX320, SRX340, SRX345, SRX550M and SRX1500 devices.
- **IRB logical interface statistics**—Interface statistics are supported on the IRB logical interface for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

To verify the IRB logical interface statistics, enter the **show interfaces irb.<index> extensive** and **show interfaces irb.<index>statistics** commands.

- **Global MAC limit**—The maximum number of MAC addresses learned on all logical interfaces on the SRX1500 device is 24,575. When this limit is reached, incoming packets with a new source MAC address will be dropped.

NAT

- When you delete or modify a NAT rule, a NAT pool, or an interface address, the related NAT bindings might not be deleted immediately. In addition, the related session scan for the NAT rule and NAT pool might not be deleted as quickly as in previous releases.
- **Source NAT pool port configuration options**—The **port-overloading-factor** option and the **port-range** option at the [edit security nat source pool *source-pool-name* port] hierarchy level can be configured together. Prior to Release 15.1X49-D40, the options would overwrite each other.

[See *port (Security Source NAT)*]

Network Management and Monitoring

- Starting with Junos OS Release 17.3R1, on SRX5400, SRX5600, and SRX5800 devices, a new option **secure-gateway** is added to the existing **request support information** command. This new option displays all the required information that is relevant for secure gateway deployment scenarios. In Junos OS Release 15.1X49-D100 and earlier, request support information displays the information about all features that might not be relevant for secure gateway deployments.
- **Enhancement to about-to-expire logic for license expiry syslog messages (SRX Series)**---As of Junos OS Release 17.3R1, the logic for multiple capacity type licenses and when their expiry raises alarms was changed. Before, the behavior had alarms and syslog messages for expiring licenses raised based on the highest validity, which would mislead users in the case of a license expiring earlier than the highest validity license. The new behavior has the about-to-expire logic based on the first expiring license.

System Logs

- The **no-tls-certificate-check** parameter is visible and disabled by default. When you enable the **no-tls-certificate-check** parameter, the Lightweight Directory Access Protocol (LDAP) server certificate will not be validated.
- On all SRX Series devices and vSRX instances, the **set security log stream \${stream_name} host \${host_IP}** command was required to configure the stream log.

Starting in Junos OS Release 15.1X49-D70, the **set security log stream \${stream_name}** command is required to configure the stream log. The source address and source interface attributes are no longer required.

Unified Threat Management (UTM)

- In Junos OS Release 15.1X49-D60 for SRX1500 devices and vSRX instances and in Junos OS Release 15.1X49-D70 for SRX4100 and SRX4200 devices:
 - The number of supported UTM policies, profiles, MIME patterns, filename extensions, and protocol commands is 500.

- The number of supported custom URL patterns and custom URL categories is 1000.

VLAN Infrastructure

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

SEE ALSO

[New and Changed Features | 204](#)

[Known Behavior | 216](#)

[Known Issues | 222](#)

[Resolved Issues | 225](#)

[Documentation Updates | 227](#)

[Migration, Upgrade, and Downgrade Instructions | 227](#)

[Product Compatibility | 231](#)

Known Behavior

IN THIS SECTION

- [Attack Detection and Prevention \(ADP\) | 217](#)
- [Class of Service | 217](#)
- [Flow-based and Packet-based Processing | 218](#)
- [General Packet Radio Service \(GPRS\) | 218](#)
- [Layer 2 Features | 219](#)
- [Multicast | 219](#)
- [Platform and Infrastructure | 220](#)
- [Software Installation and Upgrade | 220](#)
- [USB autoinstallation | 221](#)
- [VPN | 221](#)

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 17.3R1 for the SRX Series.

Attack Detection and Prevention (ADP)

- On all high-end SRX Series devices, the first path signature screen is performed first, followed by the fast path bad-inner-header screen.
- On all SRX Series devices, when a packet allow or drop session is established, the bad-inner-header screen is performed on every packet, because this screen is a fast path screen.

Class of Service

The following limitations apply to CoS support on VPN st0 interfaces:

- Currently, the maximum number for software queues is 2048. If the number of st0 interfaces exceeds 2048, not enough software queues can be created for all the st0 interfaces.
- Shaping threshold depends on two factors: interface bandwidth and shaping rate. Every interface bandwidth is received from its parent physical interface, which is divided by shaping and scheduling at the logical interface. Currently, the st0 physical interface is a pseudointerface and its maximum bandwidth is 622.08 Mbps, meaning that all of the IPsec tunnel throughput cannot exceed 622 Mbps. You must ensure that the shaping rate that you configure is smaller than its physical egress traffic.
- Only route-based VPN can apply st0 CoS. [Table 2 on page 217](#) describes the st0 CoS feature support for different types of VPN.

Table 2: CoS Feature Support for VPN

Classifier Features	Site-to-Site VPN (P2P)	ADVPN/AutoVPN (P2MP)
Classifiers, policers, and rewriting markers	Supported	Supported
Queueing, scheduling, and shaping based on st0 logical interfaces	Supported	Not supported
Queueing, scheduling, and shaping based on virtual channels	Supported	Supported

- On branch SRX Series devices, one st0 logical interface can bind to multiple VPN tunnels. The eight queues for the st0 logical interface cannot reroute the traffic to different tunnels, so pre-tunneling is not supported.

NOTE: The virtual channel feature can be used as a workaround on branch SRX Series devices.

- When defining a CoS shaping rate on an st0 tunnel interface, consider the following restrictions:
 - The shaping rate on the tunnel interface must be less than that of the physical egress interface.
 - The shaping rate only measures the packet size that includes the inner Layer 3 clear text packet with an ESP/AH header and an outer IP header encapsulation. The outer Layer 2 encapsulation added by the physical interface is not factored into the shaping rate measurement.
 - The CoS behavior works as expected when the physical interface carries the shaped GRE or IP-IP tunnel traffic only. If the physical interface carries other traffic, thereby lowering the available bandwidth for tunnel interface traffic, the CoS features do not work as expected.
- On SRX550M, SRX5400, SRX5600, and SRX5800 devices, bandwidth limit and burst size limit values in a policer configuration are a per-SPU, not per-system limitation. This is the same policer behavior as on the physical interface.

Flow-based and Packet-based Processing

- On SRX340 and SRX345 devices, fabric interfaces must be configured such that the Media Access Control Security (MACsec) configurations are local to the nodes. Otherwise, the fabric link will not be reachable.
- You can configure a security master password that allows you to encrypt shared secrets, such as RADIUS passwords and IKE preshared keys. Having a master password allows devices to encrypt passwords in such a way that only devices running Junos OS that have knowledge of the master password can decrypt the encrypted passwords. The following limitations apply:
 - The master password cannot be edited, deleted, or modified in the config-private mode.
 - For security reasons, the **deactivate system master-password** option is not supported.
 - Rolling back to a previous configuration that used a different master password is not allowed.

General Packet Radio Service (GPRS)

- Starting in Junos OS Release 15.1X49-D40, the SCTP flow session utilizes a connection tag to more finely distribute SCTP traffic across SPUs on SRX5400, SRX5600, and SRX5800 devices that support the SCTP ALG. The connection tag is decoded from the SCTP vtag. A separate SCTP session will be created for each of the first three packets—that is, one session for INIT, INIT-ACK, and COOKIE-ECHO, respectively. Because, the reverse-direction traffic has its own session, the session can no longer match the existing forward-direction session and pass through automatically. Therefore, similar to the forward-direction policy, an explicit policy is needed for approving the reverse-direction SCTP traffic.

In this scenario, the SCTP flow session requires a bidirectional policy configuration to be established for even a basic connection.

- On SRX5000 line devices, when you use the GTP inspection feature, during an ISSU from Junos OS Release 15.1X49-D10, 15.1X49-D20, or 15.1X49-D30 to Junos OS Release 15.1X49-D40 or later, GTPv0 tunnels will not be synchronized to the upgraded node.

For GTPv1 and GTPv2, the tunnels will be synchronized, but the timeout gets restarted.

Beginning with Junos OS Release 15.1X49-D40, ISSU is fully supported with the GTP inspection feature enabled.

Layer 2 Features

- The following are the limitations on SRX320, SRX340, SRX345, and SRX550M devices when configuring Ethernet connectivity fault management (CFM) over very-high-bit-rate digital subscriber line (VDSL) or Layer 3 Interface:
 - CFM Action Profiles are not supported on the Point-to-Point Protocol over Ethernet (PPPoE) logical interface.
 - Synthetic loss measurement on demand is supported. Proactive synthetic loss measurement is not supported.
 - When CFM over PPPOE is implemented, CFM should be applied on PPPoE logical interface and not on underlying interface.
 - CFM over VDSL can be implemented as Maintenance Endpoint (MEP) and not as Maintenance Intermediate Point (MIP).
 - CFM Higher level Pass-through over VDSL or Gigabit Ethernet interface in Layer 3 interface mode is not supported.
 - For vlan tagged VDSL interface, CFM should always be applied on respective logical interface and not over physical interface.
 - When CFM is enabled on VDSL, CFM packets are dropped randomly causing CFM sessions to flap based on timer when transit traffic exceeds line rate because VDSL mPIM cannot differentiate and prioritize CFM packets
- **Layer 2 Bridging and Transparent Mode**— On all SRX Series devices, bridging and transparent mode are not supported on Mini-Physical Interface Modules (Mini-PIMs).

Multicast

- On all SRX Series devices, only 100 packets can be queued during pending (S, G) route. However, when multiple multicast sessions enter the route resolve process at the same time, buffer resources are not sufficient to queue 100 packets for each session.

- On all SRX Series devices, when a multicast route is not available, pending sessions are not torn down, and subsequent packets are queued. If no multicast route resolve comes back, then the traffic flow has to wait for the pending session to timed out. Then packets can trigger new pending session create and route resolve.

Platform and Infrastructure

- On all high-end SRX Series devices, when you enable a global services offloading policy utilizing IOC2 line-cards, the connections per second (CPS) rate might be reduced. It is recommended to utilize IOC3 line-cards to maximize the CPS rate, or alternatively, lower the session count to ensure that the IOC2 is capable of scaling. As a workaround, identify the sessions that must be offloaded and only enable services offloading on those sessions.

Software Installation and Upgrade

- On SRX5000 Series devices, In-Service Software Upgrade (ISSU) is not supported for upgrading from earlier Junos OS releases to Junos OS Release 15.1X49. ISSU is supported for upgrading to successive Junos OS Release 15.1X49 releases and to major Junos OS releases.

NOTE: SRX300 Series devices and SRX550M devices do not support ISSU.

- ISSU is not supported from Junos OS Release 15.1X49 releases to 17.3, but supported from Junos OS Release 17.3 to 17.3 and up releases.

USB autoinstallation

- On SRX300 Series Services Gateways on which the USB auto-installation feature is enabled (the default configuration), removal of a USB storage device immediately after insertion is not supported.

NOTE: USB auto-installation is not supported on SRX1500 devices.

After you insert a USB storage device, Junos OS scans the device to check whether it contains the USB autoinstallation file. This process might take up to 50 seconds to complete depending on the quality of the USB storage device and the number and size of the files in the device. Removing the USB storage device while this process is running might cause the services gateway to reboot, the USB port to stop working, and data loss on the USB. We recommend that after inserting a USB storage device, you wait for at least 60 seconds before removing it.

By issuing the **set system autoinstallation usb disable** command (which disables the USB autoinstallation feature) before you insert the USB device, you can reduce the waiting interval between insertion and removal of a USB storage device from 60 seconds to 20 seconds.

VPN

- On SRX Series devices, when there are multiple traffic selectors configured for a route-based VPN, clear traffic may enter a VPN tunnel without matching a traffic selector if the IKE gateway external interface is moved to another virtual router (VR). The software does not handle the multiple asynchronous interface events generated when an IKE gateway external interface is moved to another VR. As a workaround, first deactivate the IPsec VPN tunnel and commit the configuration without that tunnel before moving the IKE gateway external interface to another VR.

SEE ALSO

[New and Changed Features | 204](#)

[Known Issues | 222](#)

[Resolved Issues | 225](#)

[Documentation Updates | 227](#)

[Migration, Upgrade, and Downgrade Instructions | 227](#)

Known Issues

IN THIS SECTION

- [Authentication and Access Control | 222](#)
- [CLI | 223](#)
- [Flow-based and Packet-based Processing | 223](#)
- [Interfaces and Chassis | 223](#)
- [J-Web | 224](#)
- [Layer 2 Ethernet Services | 224](#)
- [Platform and Infrastructure | 224](#)
- [VPNs | 224](#)

This section lists the known issues in hardware and software in Junos OS Release 17.3R1.

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

Authentication and Access Control

- For a security policy with HTTP pass-through firewall authentication being configured, we recommend that you configure web-redirect for HTTP pass-through firewall authentication instead of using direct HTTP pass-through firewall authentication because web browser may automatically carry credential in subsequential request to target web-server. [PR1230447](#)
- A user session is disconnected due to aging out of a fwauth entry in spite of an existing session. [PR1265571](#)
- In SRX device with user-fw feature, the users are sometimes not permitted to authenticate from LDAP server and get the authorized group though the group mapping.

When SRX device gets stuck in loop condition the device prevents new updates to user group mapping once it gets into an error condition. This condition occurs only when an empty user object is encountered while calculating user-group mapping. [PR1282744](#)

CLI

- SRX5400, SRX5600, and SRX5800 devices CLI hangs while displaying CA profile group. This CA profile group contains CA certificates with 100's of certificates and CLI times out as PKId needs excessive time to handle such requests. Instead of displaying entire CA group, you can display individual CA profile inside CA group to avoid this problem.

Flow-based and Packet-based Processing

- On SRX Series devices in a chassis cluster, the synchronization monitoring configuration might fail if the following configuration is enabled: set system encrypt-configuration-files. The synchronization monitoring configuration failure might result in disabling the secondary node after reboot. [PR1235628](#)
- On SRX5000 Series platforms, cold-sync will fail when SPC gets stuck and traffic loss is seen. [PR1240983](#)
- useridd may consume high CPU. Traceoptions of IUF will be full of UGCALC_AD_MEMBER_UPDATE messages. [PR1280783](#)
- On all SRX Series devices, enabling or disabling CRL download knob in CA profile does not work as expected. [PR1280530](#)
- STP change state push into PFE might fail. [PR1259286](#)

Interfaces and Chassis

- Wrong cable type is displayed for UNI-SFPs. [PR886753](#)
- On SRX1500 devices, when configuring the devices in switching mode, an IRB interface located in a custom routing-instance is not reachable. [PR1234000](#)

J-Web

- On SRX Series devices, DHCP relay configuration under Configure > Services > DHCP > DHCP Relay page is removed from J-Web. The same DHCP relay can be configured using the CLI. [PR1205911](#)

Layer 2 Ethernet Services

- VRRP MAC does not get added onto IFL mfilter hence ping to VIP address fails. If the traffic is using regular port MAC, then this issue is not seen. But any traffic are using VRRP mac, it will be dropped as the virtual MAC is not added into IFL mfilter. It only affects trio based IOC2/IOC3 cards in SRX5000 Series devices.

Platform and Infrastructure

- On SRX Series devices in a chassis cluster, if sampling is used, the flowd process fails and core files are seen on both the nodes, when route is updated through dynamic protocols, such as BGP. [PR1249254](#)

VPNs

- On SRX Series devices, if traffic-selector is configured with DPD backup gateway, the IKE redundant gateway failover fails. This may cause IPsec management daemon to restart. [PR1249908](#)
- On SRX Series devices in a chassis cluster, in a rare condition, modifying the IPsec VPN configuration might cause /var/etc/vpn_tunnel.id file mismatch between both primary node and secondary node, then the RGO failover results in the kmd process crash on the new primary node. [PR1250178](#)
- On SRX1500 devices in a chassis cluster, IP leak might occur under the following scenarios:
 - In case of IKEv1, it is possible for an IPsec VPN tunnel to be active without an active IKEv1 phase 1 SA. Since the assigned IP address associated with an IPsec VPN tunnel (for a user) is stored in the record of phase 1 SA, if HA RGO failover occurs while there is no active IKEv1 phase SA exist for an IPsec VPN tunnel, the assigned IP address will be released to the authd daemon when the IPsec VPN tunnel is disconnected.
 - In case a remote access IPsec VPN tunnel is cleared (for both IKEv1 and IKEv2), the assigned IP address is kept for 30 seconds before it is released back to the authd within an additional 2 minutes. If HA failover occurs during this time before the IP is received at the authd, there will be an IP address leak.
 - If a new IP is assigned by authd daemon after every user is authenticated, regardless of the user already having an IP assigned from an early authentication. In case of IKEv1, authentication occurs at every IKE phase 1 SA rekey. If the KMD daemon restarts immediately (within 2 minutes) after an IKEv1 phase 1 SA rekey, there is a possibility that the newly assigned IP has not been released to authd daemon yet. This will lead to the leak of that IP.

[PR1252181](#)

- On all SRX Series devices, when manual route-based IPsec VPN is configured, enabling VPN monitoring will cause the st0.* interface down, which results in VPN traffic drop. [PR1259422](#)
- Manual NHTB does not work. Following message is displayed on IKE traces, "Internal Error: Manual NHTB add failed".[PR1266797](#)
- On SRX Series devices, if traffic-selector is configured, the IKE redundant gateway failover fails. [PR1270000](#)
- On SRX5000 Series platforms, you cannot load PKI local-certificate and CA certificate with cmpv2. [PR1277317](#)
- On all SRX Series devices, CRL download fails when content-length field in http header is missing and CRL occupies at least 2 packets. [PR1278631](#)

SEE ALSO

[New and Changed Features | 204](#)

[Resolved Issues | 225](#)

[Documentation Updates | 227](#)

[Migration, Upgrade, and Downgrade Instructions | 227](#)

Resolved Issues

IN THIS SECTION

- [Interfaces and Chassis | 226](#)
- [Layer 2 Ethernet Services | 226](#)
- [Platform and Infrastructure | 226](#)
- [Routing Policy and Firewall Filters | 226](#)
- [Unified Threat Management \(UTM\) | 226](#)
- [VPNs | 226](#)

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.

Interfaces and Chassis

- On SRX1500, if software release 15.1X49-D70 or above is installed and you have a single PEM in slot 0, you will see an alarm saying PEM 1 is not present. [PR1265795](#)

Layer 2 Ethernet Services

- On SRX1500 devices, when configuring the devices to switching mode, an IRB interface located in a custom routing-instance is not reachable. [PR1234000](#)
- change the configuration set interfaces [infname] unit 0 family inet6 dhcpv6-client no-dns-propagation to set interfaces [infname] unit 0 family inet6 dhcpv6-clientno-dns-install? [PR1284852](#)

Platform and Infrastructure

- On SRX Series devices in a chassis cluster, if sampling is used, the flowd process fails and core files are seen on both the nodes, when route is updated through dynamic protocols, such as BGP. [PR1249254](#)

Routing Policy and Firewall Filters

- Starting in Junos OS Release 15.1X49-D100, a new default application, application junos-smtps, has been added for secured email traffic using port 587 or 465. To view the new default policy, use the show configuration groups junos-defaults applications command. [PR1273725](#)

Unified Threat Management (UTM)

- Some traffic from web-cam contain non-standard HTTP boundary format, it will cause SRX UTM/SAV hold traffic/mbuf, later cause failover [PR1283806](#)

VPNs

- On SRX5400, SRX5600, and SRX5800 devices, the st0 interface global counter statistics is not incrementing and keeps zero, although traffic passes through the tunnel sub-interfaces such as st0.0 and st0.1. [PR1171958](#)

SEE ALSO

[New and Changed Features | 204](#)

[Known Issues | 222](#)

[Documentation Updates | 227](#)

[Migration, Upgrade, and Downgrade Instructions | 227](#)

Documentation Updates

There are no errata or changes in Junos OS Release 17.3R1 for the SRX Series documentation.

SEE ALSO

[New and Changed Features | 204](#)

[Changes in Behavior and Syntax | 210](#)

[Known Behavior | 216](#)

[Known Issues | 222](#)

[Resolved Issues | 225](#)

[Migration, Upgrade, and Downgrade Instructions | 227](#)

[Product Compatibility | 231](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade for Layer 2 Configuration | 228](#)
- [Upgrade and Downgrade Scripts for Address Book Configuration | 228](#)

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 for Layer 2 Configuration

Starting with Junos OS Release 15.1X49-D10 and later, only enhanced Layer 2 CLI configurations are supported. If your device was configured earlier for Layer 2 transparent mode, then you must convert the legacy configurations to Layer 2 next-generation CLI configurations.

For details on how to migrate from Junos OS Release 12.3X48-D10 and earlier releases to Junos OS Release 15.1X49-D10 and later releases, refer to the Knowledge Base article at <https://kb.juniper.net/InfoCenter/index?page=content&id=KB30445>.

Upgrade and Downgrade Scripts for Address Book Configuration

IN THIS SECTION

- [About Upgrade and Downgrade Scripts | 228](#)
- [Running Upgrade and Downgrade Scripts | 230](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 230](#)

Beginning with Junos OS Release 12.1, you can configure address books under the **[security]** hierarchy and attach security zones to them (zone-attached configuration). In Junos OS Release 11.1 and earlier, address books were defined under the **[security zones]** hierarchy (zone-defined configuration).

You can either define all address books under the **[security]** hierarchy in a zone-attached configuration format or under the **[security zones]** hierarchy in a zone-defined configuration format; the CLI displays an error and fails to commit the configuration if you configure both configuration formats on one system.

Juniper Networks provides Junos operation scripts that allow you to work in either of the address book configuration formats (see [Figure 1 on page 229](#)).

About Upgrade and Downgrade Scripts

After downloading Junos OS Release 12.1, you have the following options for configuring the address book feature:

- **Use the default address book configuration**—You can configure address books using the zone-defined configuration format, which is available by default. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.
- **Use the upgrade script**—You can run the upgrade script available on the Juniper Networks support site to configure address books using the new zone-attached configuration format. When upgrading, the system uses the zone names to create address books. For example, addresses in the trust zone are

created in an address book named **trust-address-book** and are attached to the trust zone. IP prefixes used in NAT rules remain unaffected.

After upgrading to the zone-attached address book configuration:

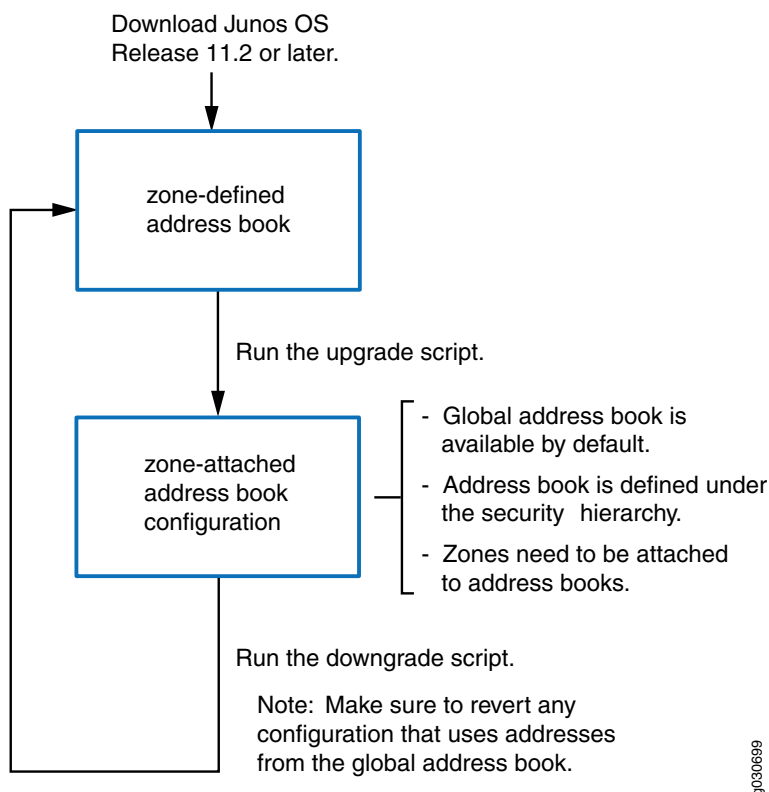
- You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.
- You cannot configure address books using the J-Web interface.

For information on how to configure zone-attached address books, see the Junos OS Release 12.1 documentation.

- **Use the downgrade script**—After upgrading to the zone-attached configuration, if you want to revert to the zone-defined configuration, use the downgrade script available on the Juniper Networks support site. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

NOTE: Before running the downgrade script, make sure to revert any configuration that uses addresses from the global address book.

Figure 1: Upgrade and Downgrade Scripts for Address Books



Running Upgrade and Downgrade Scripts

The following restrictions apply to the address book upgrade and downgrade scripts:

- The scripts cannot run unless the configuration on your system has been committed. Thus, if the zone-defined address book and zone-attached address book configurations are present on your system at the same time, the scripts will not run.
- The scripts cannot run when the global address book exists on your system.
- If you upgrade your device to Junos OS Release 12.1 and configure logical systems, the master logical system retains any previously configured zone-defined address book configuration. The master administrator can run the address book upgrade script to convert the existing zone-defined configuration to the zone-attached configuration. The upgrade script converts all zone-defined configurations in the master logical system and user logical systems.

NOTE: You cannot run the downgrade script on logical systems.

For information about implementing and executing Junos operation scripts, see the *Junos OS Configuration and Operations Automation Guide*.

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

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Release 12.3X48 is an EEOL release. You can upgrade from Junos OS Release 12.1X46 to Release 12.3X48 or even from Junos OS Release 12.3X48 to Release 15.1X49-D10. For upgrading from Junos OS Release 12.1X47-D15 to Junos OS Release 15.1X49-D10, ISSU is supported. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

For more information about EEOL releases and to review a list of EEOL releases, see <https://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 204
Changes in Behavior and Syntax 210
Known Behavior 216
Known Issues 222
Resolved Issues 225
Documentation Updates 227
Product Compatibility 231

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 231](#)

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

Changes in Behavior and Syntax 210
Known Behavior 216
Known Issues 222
Resolved Issues 225
Documentation Updates 227
Migration, Upgrade, and Downgrade Instructions 227

Upgrading Using Unified ISSU

Unified in-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic. Unified in-service software upgrade is only supported by dual Routing Engine platforms. In addition, graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) must be enabled. For additional information about using unified in-service software upgrade, see the [High Availability User Guide for Routing Devices](#).

For information about ISSU support across platforms and Junos OS releases, see the [In-Service Software Upgrade \(ISSU\)](#) Web application.

Compliance Advisor

For regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

Finding More Information

For the latest, most complete information about known and resolved issues with Junos OS, see the Juniper Networks Problem Report Search application at: <https://prsearch.juniper.net>.

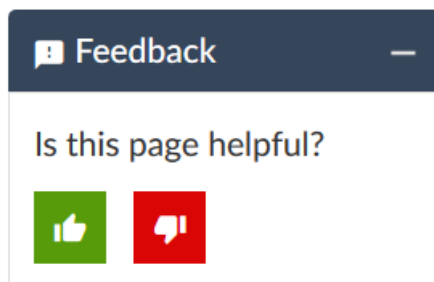
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: <https://pathfinder.juniper.net/feature-explorer/>.

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 system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://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/welcome.do>.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <https://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at <https://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

30 September 2021—Revision 19, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

3 September 2020—Revision 18, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

8 May 2020—Revision 17, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

5 December 2019—Revision 16, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

14 March 2019—Revision 15, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

14 February 2019—Revision 14, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

17 May 2018—Revision 13, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

12 April 2018—Revision 12, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

25 January 2018—Revision 11, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

14 December 2017—Revision 10, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

30 November 2017—Revision 9, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

16 November 2017—Revision 8, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

26 October 2017—Revision 7, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

23 October 2017—Revision 6, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

10 October 2017—Revision 5, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

21 September 2017—Revision 4, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

8 September 2017—Revision 3, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

1 September 2017—Revision 2, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

25 August 2017—Revision 1, Junos OS Release 17.3R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

Copyright © 2017 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.