

Release Notes

Published
2021-11-25

Junos[®] OS 19.1R1 Release Notes

SUPPORTED ON

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

HARDWARE HIGHLIGHTS

- xDSL SFP modules (NFX250)
- QFX10000-60S-6Q line card (PTX10008 and PTX10016 routers)

SOFTWARE HIGHLIGHTS

- Virtual gateway or IRB MAC addresses in a proxy ARP request (EX9200, MX Series)
- LFM support on EX2300 and EX3400 switches
- Channelize 100-Gigabit Ethernet port to four 25-Gigabit Ethernet ports in uplink module (EX4300-48MP)
- Asynchronous notification on EVPN-VPWS (MX Series)
- Abstracted Fabric interface support for MS-MPC, 16X10GE MPC, MPC2E, MPC3E, MPC4E (MX480, MX960, MX2010, MX2020, MX2008)
- In-chassis Junos Node Slicing (MX480, MX960, MX2010, and MX2020)
- MS-MIC and MS-MPC support for in-chassis Junos Node Slicing (MX480, MX960, MX2010, MX2020, MX2008)
- BGP graceful shutdown (MX Series)
- DHCP active leasequery for live updates of binding information (MX Series)

- High Availability (NFX150)
- LTE in dual CPE deployments (NFX150)
- Policy-based allocation for IPv4 BGP-labeled unicast (PTX Series, QFX Series)
- IPv4 and IPv6 inline active flow monitoring on IRB interfaces (PTX1000)
- Increasing the number of ARP and ND Entries to 256K (QFX10008 and QFX10016 switches)
- Packet load balancing based on GTP-TEID hashing (QFX10002, QFX10008, and QFX10016 switches)
- Application quality of experience (AppQoE) support in high availability (HA) mode (SRX4100, SRX4200)
- SRX TAP mode support for UTM features (SRX300, SRX320, SRX340, SRX345, SRX550HM, SRX1500, SRX4100, SRX4200, and SRX4600)
- Cryptographic algorithm support for IPsec and IKE (SRX Series)
- User firewall enhanced support for tenant systems (SRX Series)

Release Notes: Junos[®] OS Release 19.1R1 for the ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion

25 November 2021

Contents	Introduction 12
	Junos OS Release Notes for ACX Series 12
	New and Changed Features 13
	Authentication, Authorization and Accounting (AAA) (RADIUS) 13
	Platform and Infrastructure 13
	Routing Protocols 14
	Changes in Behavior and Syntax 14
	Interfaces and Chassis 15
	Network Management and Monitoring 15
	Known Behavior 16
	General Routing 16
	Known Issues 17
	General Routing 17
	Interfaces and Chassis 18
	Resolved Issues 18
	General Routing 19
	Infrastructure 20
	Services Applications 20
	Documentation Updates 21

Migration, Upgrade, and Downgrade Instructions | 21

- Upgrade and Downgrade Support Policy for Junos OS Releases | 21

Product Compatibility | 22

- Hardware Compatibility | 22

Junos OS Release Notes for EX Series Switches | 24

New and Changed Features | 24

- Hardware | 25

- Authentication, Authorization, and Accounting (AAA) | 25

- Dynamic Host Configuration Protocol | 26

- EVPNs | 26

- Interfaces and Chassis | 26

- Junos Telemetry Interface | 27

- Operation, Administration, and Maintenance (OAM) | 28

- Routing Policy and Firewall Filters | 29

- Routing Protocols | 29

- Software Installation and Upgrade | 29

Changes in Behavior and Syntax | 30

- Interfaces and Chassis | 31

- Network Management and Monitoring | 31

- Security | 31

- User Interface and Configuration | 31

Known Behavior | 32

- General Routing | 32

- Virtual Chassis | 33

Known Issues | 33

- General Routing | 34

- Infrastructure | 35

- Interfaces and Chassis | 35

- Junos Fusion Enterprise | 35

- Layer 2 Features | 36

- Multicast | 36

- Network Management and Monitoring | 36

- Platform and Infrastructure | 36

- Routing Protocols | 36

Subscriber Access Management	37
Resolved Issues	37
EVPN	38
General Routing	38
Infrastructure	39
Junos Fusion Enterprise	39
Layer 2 Features	40
Layer 3 Features	40
Platform and Infrastructure	40
Routing Protocols	40
Documentation Updates	41
Migration, Upgrade, and Downgrade Instructions	42
Upgrade and Downgrade Support Policy for Junos OS Releases	42
Product Compatibility	43
Hardware Compatibility	43
Junos OS Release Notes for Junos Fusion Enterprise	44
New and Changed Features	44
Junos Fusion Enterprise	45
Changes in Behavior and Syntax	45
Known Behavior	46
Known Issues	46
Resolved Issues	47
Junos Fusion Enterprise	47
Documentation Updates	48
Migration, Upgrade, and Downgrade Instructions	48
Basic Procedure for Upgrading Junos OS on an Aggregation Device	49
Upgrading an Aggregation Device with Redundant Routing Engines	51
Preparing the Switch for Satellite Device Conversion	51
Converting a Satellite Device to a Standalone Switch	52
Upgrade and Downgrade Support Policy for Junos OS Releases	53
Downgrading from Junos OS	53
Product Compatibility	54
Hardware and Software Compatibility	54
Hardware Compatibility Tool	54

Junos OS Release Notes for Junos Fusion Provider Edge | 55

New and Changed Features | 55

Authentication, Authorization and Accounting (AAA) (RADIUS) | 56

Changes in Behavior and Syntax | 56

Known Behavior | 57

Known Issues | 57

Resolved Issues | 58

Junos Fusion Provider Edge | 58

Junos Fusion Satellite Software | 58

Documentation Updates | 59

Migration, Upgrade, and Downgrade Instructions | 59

Basic Procedure for Upgrading an Aggregation Device | 60

Upgrading an Aggregation Device with Redundant Routing Engines | 62

Preparing the Switch for Satellite Device Conversion | 63

Converting a Satellite Device to a Standalone Device | 64

Upgrading an Aggregation Device | 66

Upgrade and Downgrade Support Policy for Junos OS Releases | 67

Downgrading from Junos OS Release 19.1 | 67

Product Compatibility | 68

Hardware Compatibility | 68

Junos OS Release Notes for MX Series 5G Universal Routing Platform | 69

New and Changed Features | 69

Release 19.1R1-S1 New and Changed Features | 70

Release 19.1R1 New and Changed Features | 70

Changes in Behavior and Syntax | 90

EVPN | 91

General Routing | 91

Interfaces and Chassis | 91

MPLS | 93

Network Management and Monitoring | 94

Network Operations and Troubleshooting Automation | 94

Routing Protocols | 94

Services Applications | 94

Software-Defined Networking (SDN) | 95

Subscriber Management and Services	95
User Interface and Configuration	95
Known Behavior	96
Forwarding and Sampling	96
General Routing	96
Infrastructure	97
MPLS	97
Platform and Infrastructure	97
Routing Protocols	97
Software Defined Networking	97
Subscriber Management and Services	98
Known Issues	99
EVPN	99
Forwarding and Sampling	99
General Routing	100
Infrastructure	105
Interfaces and Chassis	105
Layer 2 Ethernet Services	106
MPLS	106
Network Management and Monitoring	107
Platform and Infrastructure	107
Routing Policy and Firewall Filters	107
Routing Protocols	107
Subscriber Access Management	109
User Interface and Configuration	109
VPNs	109
Resolved Issues	110
Resolved Issues: 19.1R1	110
Documentation Updates	123
Spanning Tree Protocol User Guide	123
Migration, Upgrade, and Downgrade Instructions	123
Basic Procedure for Upgrading to Release 19.1	124
Procedure to Upgrade to FreeBSD 11.x based Junos OS	125
Procedure to Upgrade to FreeBSD 6.x based Junos OS	127

Upgrade and Downgrade Support Policy for Junos OS Releases	129
Upgrading a Router with Redundant Routing Engines	129
Downgrading from Release 19.1	130
Product Compatibility	130
Hardware Compatibility	130
Junos OS Release Notes for NFX Series	131
New and Changed Features	132
What's New in Release 19.1R1	132
Changes in Behavior and Syntax	134
Known Behavior	135
High Availability (HA)	135
Known Issues	136
Security	136
Performance Modes	136
Resolved Issues	137
Resolved Issues: 19.1R1	137
Documentation Updates	138
Migration, Upgrade, and Downgrade Instructions	138
Upgrade and Downgrade Support Policy for Junos OS Releases	139
Basic Procedure for Upgrading to Release 19.1	139
Product Compatibility	141
Hardware Compatibility	141
Junos OS Release Notes for PTX Series Packet Transport Routers	143
New and Changed Features	144
Hardware	144
Authentication, Authorization, and Accounting (AAA)	145
Class of Service	145
Forwarding and Sampling	145
Junos Telemetry Interface	146
Layer 3 Features	148
MPLS	149
Multicast	151
Network Management and Monitoring	151
Routing Policy and Firewall Filters	152

Routing Protocols	152
Services Applications	154
Changes in Behavior and Syntax	155
Interfaces and Chassis	156
Network Management and Monitoring	156
Services Applications	157
User Interface and Configuration	157
Known Behavior	158
General Routing	158
Known Issues	159
General Routing	159
Interfaces and Chassis	161
Routing Protocols	161
Resolved Issues	161
General Routing	162
Interfaces and Chassis	163
MPLS	163
Platform and Infrastructure	163
Routing Protocols	164
Documentation Updates	164
Migration, Upgrade, and Downgrade Instructions	165
Basic Procedure for Upgrading to Release 19.1	165
Upgrade and Downgrade Support Policy for Junos OS Releases	168
Upgrading a Router with Redundant Routing Engines	168
Product Compatibility	169
Hardware Compatibility	169
Junos OS Release Notes for the QFX Series	170
New and Changed Features	170
Hardware	172
Authentication, Authorization and Accounting (AAA) (RADIUS)	172
Class of Service (CoS)	172
EVPNs	173
Forwarding and Sampling	173
General Routing	174

Interfaces and Chassis	177
Junos Telemetry Interface	178
Layer 2 Features	179
Licensing	179
Management	180
MPLS	180
Network Management and Monitoring	181
Routing Policy and Firewall Filters	182
Routing Protocols	182
System Management	184
Changes in Behavior and Syntax	184
Interfaces and Chassis	185
Network Management and Monitoring	186
Security	186
User Interface and Configuration	186
Known Behavior	187
EVPN	187
Layer 2 Features	187
MPLS	188
Platform and Infrastructure	188
Routing Protocols	189
Virtual Chassis	189
Known Issues	189
EVPN	190
General Routing	190
Layer 2 Features	191
MPLS	191
Platform and Infrastructure	191
Routing Protocols	194
Resolved Issues	195
EVPN	195
Interfaces and Chassis	196
Layer 2 Ethernet Services	196
Layer 2 Features	196

MPLS	197
Network Management and Monitoring	197
Platform and Infrastructure	197
Routing Protocols	200
Documentation Updates	200
Migration, Upgrade, and Downgrade Instructions	201
Upgrading Software on QFX Series Switches	201
Installing the Software on QFX10002-60C Switches	204
Installing the Software on QFX10002 Switches	204
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	205
Installing the Software on QFX10008 and QFX10016 Switches	207
Performing a Unified ISSU	211
Preparing the Switch for Software Installation	212
Upgrading the Software Using Unified ISSU	212
Upgrade and Downgrade Support Policy for Junos OS Releases	214
Product Compatibility	215
Hardware Compatibility	215
Junos OS Release Notes for SRX Series	216
New and Changed Features	217
Application Security	218
Authentication Access Control	219
Intrusion Detection and Prevention (IDP)	219
J-Web	220
Logical Systems and Tenant Systems	225
Routing Policy and Firewall Filters	226
Routing Protocols	226
Security	226
Unified Threat Management (UTM)	226
VPN	227
Changes in Behavior and Syntax	229
Flow-Based and Packet-Based Processing	230
Network Management and Monitoring	230
Platform and Infrastructure	230

User Interface and Configuration	230
VPN	230
Known Behavior	231
Application Security	232
Flow-Based and Packet-Based Processing	232
J-Web	232
Interfaces and Chassis	232
Platform and Infrastructure	232
Known Issues	233
Application Layer Gateways (ALGs)	233
Chassis Clustering	233
Flow-Based and Packet-Based Processing	234
J-Web	234
VPNs	235
Resolved Issues	235
Application Security	236
Application Layer Gateways (ALGs)	236
Chassis Clustering	236
Flow-Based and Packet-Based Processing	236
Integrated User Firewall	238
Interfaces and Routing	238
Intrusion Detection and Prevention (IDP)	238
Installation and Upgrade	238
J-Web	238
Layer 2 Ethernet Services	239
Multiprotocol Label Switching (MPLS)	239
Network Address Translation (NAT)	239
Platform and Infrastructure	239
Routing Policy and Firewall Filters	240
Routing Protocols	240
Services Applications	240
Software Installation and Upgrade	240
Unified Threat Management (UTM)	240
VPNs	240

Documentation Updates | 241

Migration, Upgrade, and Downgrade Instructions | 242

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 242

Product Compatibility | 243

Hardware Compatibility | 243

Upgrading Using ISSU | 244

Licensing | 244

Compliance Advisor | 244

Finding More Information | 245

Documentation Feedback | 245

Requesting Technical Support | 246

Self-Help Online Tools and Resources | 246

Creating a Service Request with JTAC | 247

Revision History | 247

Introduction

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

These release notes accompany Junos OS Release 19.1R1 for the ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Junos OS Release Notes for ACX Series

IN THIS SECTION

- New and Changed Features | 13
- Changes in Behavior and Syntax | 14
- Known Behavior | 16
- Known Issues | 17
- Resolved Issues | 18
- Documentation Updates | 21
- Migration, Upgrade, and Downgrade Instructions | 21
- Product Compatibility | 22

These release notes accompany Junos OS Release 19.1R1 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- [Authentication, Authorization and Accounting \(AAA\) \(RADIUS\) | 13](#)
- [Platform and Infrastructure | 13](#)
- [Routing Protocols | 14](#)

This section describes the new features and enhancements to existing features in Junos OS Release 19.1R1 for ACX Series Universal Metro Routers.

Authentication, Authorization and Accounting (AAA) (RADIUS)

- **Support for SFTP global disablement (ACX Series)**—Starting in Junos OS Release 19.1R1, we have globally disabled incoming SSH File Transfer Protocol (SFTP) connections by default. You can enable incoming SFTP connections globally by configuring the statement **sftp-server** at the **[edit system services ssh]** hierarchy level. Prior to Junos OS Release 19.1R1, the incoming SFTP connections were globally enabled by default.

[See [Configuring sftp-server](#)]

Platform and Infrastructure

- **DMA recovery mechanism (ACX Series)**—A recovery mechanism has been introduced that is triggered in case the router enters an Idle state on any DMA channels. The recovery mechanism reboots the Packet Forwarding Engine to recover from Idle state.

The following recovery message is logged in the Routing Engine syslog message:

```
CHASSISD_FPC_ASIC_ERROR: <FPC 0> ASIC Error detected errorno 0x0000ffff FPC
restart initiated
```

The following recovery message is logged in the Packet Forwarding Engine syslog message:

```
BCM DMA channel error detected
Resetting the PFE
```

Routing Protocols

- **Support for BGP graceful shutdown (ACX Series)**— Starting in Junos OS Release 19.1R1, graceful traffic migration from one BGP next hop to another is supported, without traffic interruption. Also, BGP administrative shutdown communication can be sent to the BGP peer.

You can configure both **graceful-shutdown** and **shutdown** statements at the `[edit protocols bgp]`, `[edit protocols bgp group group-name]`, and `[edit protocols bgp group group-name neighbor address]` hierarchy levels.

NOTE: Graceful shutdown is disabled by default.

[See: [graceful-shutdown \(Protocols BGP\)](#), [shutdown \(Protocols BGP\)](#).]

SEE ALSO

Changes in Behavior and Syntax	14
Known Behavior	16
Known Issues	17
Resolved Issues	18
Documentation Updates	21
Migration, Upgrade, and Downgrade Instructions	21
Product Compatibility	22

Changes in Behavior and Syntax

IN THIS SECTION

- [Interfaces and Chassis](#) | [15](#)
- [Network Management and Monitoring](#) | [15](#)

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 19.1R1 for the ACX Series routers.

Interfaces and Chassis

- **Support for creating layer 2 logical interface independently (ACX Series)**—In Junos OS Releases 18.4R1, 18.4R2, 19.1R1, 19.1R2, and later, ACX Series routers support creating Layer 2 logical interface independent of Layer 2 routing instance type. That is, you can configure and commit the Layer 2 logical interfaces separately and add the interface to bridge-domain or Ethernet VPN (EVPN) routing instance separately. Note that the Layer 2 logical interfaces works fine only when the interface is added to bridge domain or EVPN routing instance.

In the earlier Junos OS releases, when a Layer 2 logical interface configuration (units with encapsulation vlan-bridge configuration) is used, then the logical interface must be added as part of a bridge-domain or EVPN routing instance for the commit to succeed.

Network Management and Monitoring

- **NETCONF <kill-session> operation returns different values in <rpc-error> when the session identifier is equal to the current session ID (ACX Series)**—Starting in Junos OS Release 19.1R1, when you execute the <kill-session> NETCONF operation and the session identifier is equal to the current session ID, the values of the <error-type> and <error-tag> elements in the resulting <rpc-error> are **application** and **invalid-value**, respectively. In earlier releases, the <error-type> and <error-tag> values are **protocol** and **operation-failed**.

[See [<kill-session>](#).]

SEE ALSO

New and Changed Features 13
Known Behavior 16
Known Issues 17
Resolved Issues 18
Documentation Updates 21
Migration, Upgrade, and Downgrade Instructions 21
Product Compatibility 22

Known Behavior

IN THIS SECTION

- [General Routing | 16](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 19.1R1 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.

General Routing

- ARP learning rate is very low. [PR1343221](#)
- Telemetry infrastructure on the ACX6360-OR and ACX6360-OX does not support interface filtering capability. Therefore, when you enable a particular sensor for telemetry, it is enabled for all the interfaces. [PR1371996](#)
- For the et interface, only a PRE_FEC_SD defect will be raised No OTN alarm will be raised. [PR1371997](#)
- The "static-cak" encryption does not work between two ACX-OX transponder nodes. [PR1389802](#)
- For the ACX6360 TIC, we only have 8 ports, so the following commands need to be corrected:
`user@router> request chassis beacon fpc 0 pic-slot 1 port 15 on FPC 0 PIC 1 PORT 15 ON user@router> show chassis beacon fpc 0 pic-slot 1 port-range lower-limit 0 upper-limit 15 FPC 0 PIC 1 PORT 0 ON FPC 0 PIC 1 PORT 1 ON FPC 0 PIC 1 PORT 2 ON FPC 0 PIC 1 PORT 3 ON FPC 0 PIC 1 PORT 4 ON FPC 0 PIC 1 PORT 5 ON FPC 0 PIC 1 PORT 6 ON FPC 0 PIC 1 PORT 7 ON FPC 0 PIC 1 PORT 8 ON FPC 0 PIC 1 PORT 9 ON FPC 0 PIC 1 PORT 10 OFF FPC 0 PIC 1 PORT 11 OFF FPC 0 PIC 1 PORT 12 OFF FPC 0 PIC 1 PORT 13 OFF FPC 0 PIC 1 PORT 14 OFF FPC 0 PIC 1 PORT 15 ON.` [PR1399335](#)

SEE ALSO

New and Changed Features 13
Changes in Behavior and Syntax 14
Known Issues 17
Resolved Issues 18
Documentation Updates 21

Known Issues

IN THIS SECTION

- [General Routing | 17](#)
- [Interfaces and Chassis | 18](#)

This section lists the known issues in hardware and software in Junos OS Release 19.1R1 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.

General Routing

- When the ACX2100 and ACX2200 are used as ingress PE routers for L2circuit connections, and the PE-CE interface (UNI) is an aggregated Ethernet interface, then upon MPLS path switchover, the traffic might be silently dropped or discarded. [PR1194551](#)
- In an earlier scenario where only the PCS is down and PMD is up, the status is not sent to the MAC and hence interrupt is not generated. However, the status will be picked up as part of the 1-second periodic and hence the link will go down for a second. Now, in spite of taking the link status from the MAC, we read the PHY status to avoid the intermittent link down status observed in the PCS. [PR1223457](#)
- START_BY_START_ERR interrupt handler was not available with the previous version of bcm sdk code. This led to the status checking of this flag continuously by bcmDPC process, leading to high CPU utilization. A handler for this interrupt should be added. [PR1329656](#)
- ACX5448: When 1-gigabit SFP is plugged in the router, autonegotiation is enabled by default. There is no functional impact. Only the CLI **show interfaces <intf-name> extensive** command output will show the autonegotiation field as disabled. [PR1343679](#)
- On the ACX5000, in Junos OS Release 17.3 and later release, the Packet Forwarding Engine syslog frequently shows the following error message: **acx_cos_tcp_bind_queues:736 parent acx_cos_tcp_ifd for ifd:ae0 does not exist for ifl:549**. In Release 17.3R3-S1, the error logs appear only from time to time, and this can be related with to an interface flap. In Release 18.1R3, the logs appear constantly, without any interface flap. This message is related to HCOS checking (even without HCOS configured). In the

- software fix, we should check if the aggregated interface has HCOS configured or not. If not, we should return gracefully from this function without throwing this error. This is a harmless message. [PR1392088](#)
- CFM adjacency is not going down with distinct intervals. [PR1397883](#)
 - Explicit swap-push map operations are now introduced on VPLS logical interfaces in ACX5000. This is already supported as part of implicit map operations or routing instance-level configurations. [PR1398118](#)
 - A jnxIfOtnOperState trap notification is sent for all ot interfaces. This is a day-1 issue. [PR1406758](#)

Interfaces and Chassis

- When an unnumbered interface is binding to an interface which has more than one IP address and one of the IPs is deleted, the family inet of the unnumbered interface might be getting deleted. The issue results in traffic loss for all the services that rely on the family inet of the unnumbered interface. Configure **preferred-source-address** on the unnumbered interface will prevent deletion of the IP hence, avoiding the deletion of the family inet of the unnumbered interface. [PR1412534](#)

SEE ALSO

New and Changed Features 13
Changes in Behavior and Syntax 14
Known Behavior 16
Resolved Issues 18
Documentation Updates 21
Migration, Upgrade, and Downgrade Instructions 21
Product Compatibility 22

Resolved Issues

IN THIS SECTION

- [General Routing | 19](#)
- [Infrastructure | 20](#)
- [Services Applications | 20](#)

This section lists the issues fixed in Junos OS Release 19.1R1 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.

General Routing

- SNMP MIB walk/get/set on jnxDomCurrentTable and jnxDomNotifications might fail on ACX platforms. [PR1076943](#)
- ACX Series routers support from dual-tagged through untagged packets Layer 3 traffic. [PR1307666](#)
- ACX5000: fpc0 acx_rt_ip_uc_lpm_install:LPM route add failed error Reason: Invalid parameter after configuring lpm-profile. [PR1365034](#)
- VPLS with **vlan-id-list** is not working properly in some releases when the link between a PE device and a CE device is an aggregated Ethernet interface with a single member link and child physical interface flap. [PR1365894](#)
- **LIBCOS_COS_TVP_FC_INFO_NOT_FOUND: Forwarding-class information not specified** prints while commit on configuration prompt. [PR1376665](#)
- On ACX5448, channelized ET interface of 25-Gigabit Ethernet interface will not come up after chassis-control restart. [PR1379288](#)
- The L2circuit might stop forwarding traffic when core interface flapping happens. [PR1381487](#)
- Timestamp is incorrect for BER statistics after clearing. [PR1386253](#)
- The **request chassis beacon** CLI command is not working for PIC slot 1 (that is, CFP2 ports). [PR1386711](#)
- ACX 5448:100-Gigabit link FEC is enabled by default on 100-Gigabit LR4. [PR1389518](#)
- On ACX Series platforms, the **forwarding-option dhcp-relay forward-only** command stops working and the DHCP packets are dropped. [PR1392261](#)
- Certain builds of Junos OS do not allow you to upgrade or commit configuration changes when the SI service interface is used. [PR1393729](#)
- [ACX] MTU is not properly applied, and the output ping mpls l2circuit sweep is giving lower values than expected. [PR1393947](#)
- This model of egress VPLS filter and the output of with "physical-interface-specific" semantic is only to be used to cater to use cases where there is a need to install a "physical-port-based" filter in the egress firewall. [PR1395362](#)
- ACX5048 RPM RFC 2544 benchmarking test is failing to start. [PR1395730](#)
- Error message **ACX_PFE_ERROR: dnx_cfm_bd_endpoint_create: Failed to destroy the remote endpoint, Endpoint id 0x2001001, Entry not found** been logged. [PR1397878](#)
- Error message **ACX_ASIC_PROGRAMMING_ERROR: dnx_cfm_bd_endpoint_create: Failed to create the local endpoint Invalid parameter** been logged on peer node. [PR1397951](#)

- **Output packet error Count** is 40-Gigabit Ethernet and 100-Gigabit Ethernet ports. [PR1398270](#)
- High jsd or na-grpcd CPU usage might be seen even if JET or JTI is not used. [PR1398398](#)
- Dynamic tunnels are not supported on ACX Series routers. [PR1398729](#)
- ACX5448: Not able to configure bridge domain more than 1024, using 100-Gigabit and aggregated Ethernet interface in BD. [PR1399214](#)
- FPC might crash after offline/online MIC-3D-16CHE1-T1-CE-H. [PR1402563](#)
- ACX5448 supports TrTCM policer configuration parameters of RFC 4115. [PR1405798](#)
- aggregated Ethernet interface TWAMP history statistics verification on client is not getting expected "Request Timed Out" error. [PR1411344](#)
- Number of inet-arp policers implemented on ACX5000 has been increased from 16 to 64. [PR1413807](#)
- Swap memory is not initialized on boot on ACX5048. [PR1415898](#)

Infrastructure

- The error of **jlaunchd: disk-monitoring is thrashing, not restarted** might be seen. [PR1380032](#)

Services Applications

- The spd might crash when **any-ip** is configured in the from clause of the NAT rule with the static translation type. [PR1391928](#)

SEE ALSO

[New and Changed Features | 13](#)

[Changes in Behavior and Syntax | 14](#)

[Known Behavior | 16](#)

[Known Issues | 17](#)

[Documentation Updates | 21](#)

[Migration, Upgrade, and Downgrade Instructions | 21](#)

[Product Compatibility | 22](#)

Documentation Updates

There are no errata or changes in Junos OS Release 19.1R1 documentation for the ACX Series.

SEE ALSO

- [New and Changed Features | 13](#)
- [Changes in Behavior and Syntax | 14](#)
- [Known Behavior | 16](#)
- [Known Issues | 17](#)
- [Resolved Issues | 18](#)
- [Migration, Upgrade, and Downgrade Instructions | 21](#)
- [Product Compatibility | 22](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 21](#)

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1,

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

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

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

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

SEE ALSO

New and Changed Features 13
Changes in Behavior and Syntax 14
Known Behavior 16
Known Issues 17
Resolved Issues 18
Documentation Updates 21
Product Compatibility 22

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 22](#)

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://apps.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	 13
Changes in Behavior and Syntax	 14
Known Behavior	 16
Known Issues	 17
Resolved Issues	 18
Documentation Updates	 21
Migration, Upgrade, and Downgrade Instructions	 21

Junos OS Release Notes for EX Series Switches

IN THIS SECTION

- New and Changed Features | 24
- Changes in Behavior and Syntax | 30
- Known Behavior | 32
- Known Issues | 33
- Resolved Issues | 37
- Documentation Updates | 41
- Migration, Upgrade, and Downgrade Instructions | 42
- Product Compatibility | 43

These release notes accompany Junos OS Release 19.1R1 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- Hardware | 25
- Authentication, Authorization, and Accounting (AAA) | 25
- Dynamic Host Configuration Protocol | 26
- EVPNs | 26
- Interfaces and Chassis | 26
- Junos Telemetry Interface | 27
- Operation, Administration, and Maintenance (OAM) | 28
- Routing Policy and Firewall Filters | 29

- Routing Protocols | 29
- Software Installation and Upgrade | 29

This section describes the new features and enhancements to existing features in Junos OS Release 19.1R1 for the EX Series.

NOTE: The following EX Series switches are supported in Release 19.1R1: EX2300, EX3400, EX4300, EX4600-40F, EX4650, EX9200, EX9204, EX9208, EX9214, EX9251, and EX9253.

Hardware

- **Support for SFP transceivers on 4-port 10GbE uplink module for EX4300-48MP and EX4300-48MP-S switches**—Starting with Junos OS Release 19.1R1, the 4-port 10GbE uplink module for EX4300-48MP and EX4300-48MP-S switches support SFP transceivers. You do not need to configure 1-Gbps speed on the uplink module to support SFP transceivers; it automatically detects the transceiver and creates the interface accordingly.

[See [EX4300 Switch Hardware Guide](#).]

Authentication, Authorization, and Accounting (AAA)

- **RADIUS over TLS (using RADsec) support (EX4300 switches)**—Starting in Junos OS Release 19.1R1, RADsec is supported for EX4300 switches. The RADsec protocol provides secure transport of RADIUS authentication and accounting data across untrusted networks using Transport Layer Security (TLS) over TCP as the transport protocol.

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

- **Support for SFTP global disablement (EX Series)**—Starting in Junos OS Release 19.1R1, we have globally disabled incoming SSH File Transfer Protocol (SFTP) connections by default. You can enable incoming SFTP connections globally by configuring the statement **sftp-server** at the **[edit system services ssh]** hierarchy level. Prior to Junos OS Release 19.1R1, the incoming SFTP connections were globally enabled by default.

[See [Configuring sftp-server](#).]

Dynamic Host Configuration Protocol

- **Increased number of DHCP relay servers supported (EX9200 switches)**—Starting in Junos OS Release 19.1R1, server groups can include up to 32 active server IP addresses in a DHCPv4 or DHCPv6 relay configuration.

[See [Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups](#).]

EVPNs

- **Support for proxy MAC addresses in an ARP request (EX9200)**—Starting in Junos OS Release 19.1R1, provider edge (PE) devices in an EVPN network that support ARP proxy can use a proxy MAC address in the ARP replies message to a host. When a PE device receives an ARP request or NDP request, it searches its MAC-IP address binding database for the requested IP address. If the device finds the MAC-IP address entry in its database, it responds to the request with the proxy MAC address. The proxy MAC address is derived from the IRB interface in an EVPN network with edge-routed bridging overlay and from the manually configured MAC address in a centrally-routed bridging overlay. If the device does not find an entry, the PE device replaces the MAC and IP address from the CE device in the ARP request with the proxy MAC and IP address of the IRB interface. This allows for enhanced security (i.e. L3 filtering) deployments on L3 gateway for both inter-VLAN and intra-VLAN traffic will be routed.

To enable this feature, configure the **proxy-mac [irb | proxy-mac-address]** statement at the **[edit routing-instances routing-instance-name protocols evpn]** hierarchy or at the **[edit routing-instances routing-instance-name bridge-domains domain_name]** hierarchy.

[See [ARP and NDP Request with a proxy MAC address](#).]

- **EVPN-VXLAN support (EX4300-48MP switches)**—Starting in Junos OS Release 19.1R1, the EX4300-48MP switch, which functions as a Layer 2 VXLAN gateway in an EVPN-VXLAN network, supports the following features:
 - Multihoming active/active
 - Proxy ARP use and ARP suppression, and NDP use and NDP suppression on non-IRB interfaces
 - Ingress node replication for broadcast, unknown unicast, and multicast (BUM) traffic forwarding

[See [EVPN User Guide](#).]

Interfaces and Chassis

- **Support for 1-Gbps speed on 4-port 1-Gigabit Ethernet/10-Gigabit Ethernet uplink module (EX4300-48MP)**—Starting with Junos OS Release 19.1R1, the 4-port 1-Gigabit Ethernet/10-Gigabit Ethernet uplink module (EX-UM-4SFPP-MR) on EX4300-48MP switches supports 1-Gbps speed. You

do not need to explicitly configure 1-Gbps speed on the uplink module, because it automatically identifies the installed 1-Gigabit SFP transceivers and creates the interface accordingly.

NOTE: The status LED of the 1-Gigabit Ethernet uplink module port is solid green (instead of blinking green) because of a device limitation. However, there is no impact on device functionality.

[See [speed \(Ethernet\)](#).]

- **Support to channelize 100-Gigabit Ethernet port to four 25-Gigabit Ethernet ports in uplink module (EX4300-48MP)**—Starting with Junos OS Release 19.1R1, in the 2-port QSFP+/1-port QSFP28 uplink module on EX4300-48MP switches, you can channelize the 100-Gigabit Ethernet port to operate as four independent 25-Gigabit Ethernet ports by using breakout cables.

[See [Setting the Mode on 2-port QSFP+/1-port QSFP28 Uplink Module \(CLI Procedure\)](#).]

- **Improved performance of small packets (EX Series)**—Starting in Junos OS Release 19.1R1, the EX9200-40XS and EX9200-12QS line cards provide improved performance of small packets (with a minimum packet size of 64 bytes) in transmit direction. To enable this feature, reduce the number of active ports (at the PIC level) to the following maximum numbers:
 - Sixteen 10-Gbps ports
 - Four 40-Gbps ports
 - Two 100-Gbps ports (when the line card is in 240-Gbps mode)
 - Three 100-Gbps ports (when the line card is in 400-Gbps mode)

To configure the number of active ports, use the existing command **set chassis fpc slot pic slot number-of-ports number-of-active-ports**.

NOTE: The command does not change packet performance at the Packet Forwarding Engine level; it improves packet performance in transmit direction at the port level only.

Junos Telemetry Interface

- **Export of data associated with the Junos kernel through Junos Telemetry Interface (JTI) (EX9200, EX9251, and EX9253)**—Starting in Junos OS Release 19.1R1, you can export data associated with the Junos kernel through remote procedure calls (gRPC) and JTI. Kernel telemetry data includes information on Veriexec state, graceful Routing Engine switchover (GRES), in-service software upgrade (ISSU), and Routing Engine ifstate. Junos kernel sensors can be used by device monitoring and network analytics applications to provide insight into the health status of the Junos kernel.

Junos kernel sensors introduced in Junos OS Release 19.1R1 support both periodical and ON_CHANGE streaming. The following Junos kernel resource paths support periodical streaming only:

- /junos/kernel-ifstate/dead-ifstates-cnt
- /junos/kernel-ifstate/alive-ifstates-cnt
- /junos/kernel-ifstate/delayed-unrefs-cnt
- /junos/kernel-ifstate/delayed-unrefs-max

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

Operation, Administration, and Maintenance (OAM)

- **LFM support on EX2300 and EX3400 switches** —Starting with Junos OS Release 19.1R1, OAM link fault management (LFM) is supported on EX2300 and EX3400 switches. OAM LFM can be configured on point-to-point Ethernet links that are connected directly or through Ethernet repeaters, and on aggregated Ethernet interfaces. The LFM status of individual links determines the LFM status of the aggregated Ethernet interface. The following OAM LFM features are supported:
 - Discovery and link monitoring
 - Remote fault detection
 - Remote loopback

[See [IEEE 802.3ah OAM Link-Fault Management Overview](#).]

Routing Policy and Firewall Filters

- **Support for matching IPv6 source addresses from an inet6 egress interface (EX4300)**—Starting in Junos OS Release 19.1R1, you can configure an firewall filter on a IPv6 egress interface to match specified IPv6 source or destination addresses, for example, to protect a third-party device connected to the switch.

[See [eracl-ip6-match](#) and [Example: Configuring an Egress Filter Based on IPv6 Source or Destination IP Addresses](#).]

Routing Protocols

- **Support for BGP graceful shutdown (EX Series)**— Starting in Junos OS Release 19.1R1, graceful traffic migration from one BGP next hop to another is supported, without traffic interruption. Also, BGP administrative shutdown communication can be sent to the BGP peer.

You can configure both **graceful-shutdown** and **shutdown** statements at the **[edit protocols bgp]**, **[edit protocols bgp group group-name]**, and **[edit protocols bgp group group-name neighbor address]** hierarchy levels.

NOTE: Graceful shutdown is disabled by default.

[See: [graceful-shutdown \(Protocols BGP\)](#), [shutdown \(Protocols BGP\)](#).]

Software Installation and Upgrade

- **Phone-home client (EX4300-MP switches)**—Starting with Junos OS Release 19.1R1, you can use either the legacy DHCP-options-based ZTP or the phone-home client (PHC) to provision software for the switch. If the switch boots up and there are DHCP options received from the DHCP server for ZTP, ZTP resumes. If DHCP options are not present, PHC is attempted. PHC enables the switch to securely obtain bootstrapping data, such as a configuration or software image, with no user intervention other than having to physically connect the switch to the network. When the switch first boots, PHC connects to a redirect server, which will redirect to a phone home server to get the configuration or software image.

To initiate either DHCP-options-based ZTP or PCH, the switch must either be in a factory-default state, or you can issue the **request system zeroize** command.

[See [Understanding the Phone-Home Client](#).]

- **Phone-home client (EX2300-MP switches)**—Starting with Junos OS Release 19.1R1, you can use either the legacy DHCP-options-based ZTP or the phone-home client (PHC) to provision software for the

switch. If the switch boots up and there are DHCP options received from the DHCP server for ZTP, ZTP resumes. If DHCP options are not present, PHC is attempted. PHC enables the switch to securely obtain bootstrapping data, such as a configuration or software image, with no user intervention other than having to physically connect the switch to the network. When the switch first boots, PHC connects to a redirect server, which will redirect to a phone home server to get the configuration or software image. To initiate either DHCP-options-based ZTP or PCH, the switch must either be in a factory-default state, or you can issue the **request system zeroize** command.

[See [Understanding the Phone-Home Client.](#)]

SEE ALSO

Changes in Behavior and Syntax	 30
Known Behavior	 32
Known Issues	 33
Resolved Issues	 37
Documentation Updates	 41
Migration, Upgrade, and Downgrade Instructions	 42
Product Compatibility	 43

Changes in Behavior and Syntax

IN THIS SECTION

- [Interfaces and Chassis](#) | [31](#)
- [Network Management and Monitoring](#) | [31](#)
- [Security](#) | [31](#)
- [User Interface and Configuration](#) | [31](#)

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 19.1R1 for the EX Series.

Interfaces and Chassis

- **No support for performance monitoring on AE Interfaces (EX4300)**—Y.1731 performance monitoring (PM) over aggregated Ethernet interfaces is not supported on EX4300 switches. [See [sla-iterator-profile](#).]
- **Support for creating Layer 2 logical interfaces independently (EX Series)**—In Junos OS Releases 18.4R1, 18.4R2, 19.1R1, 19.1R2, and later, EX Series switches support creating Layer 2 logical interfaces independent of Layer 2 routing instance type. That is, you can configure and commit the Layer 2 logical interfaces separately and add the interface to the bridge domain or Ethernet VPN (EVPN) routing instance separately. Note that the Layer 2 logical interfaces works fine only when the interface is added to the bridge domain or EVPN routing instance.

In the earlier Junos OS releases, when a Layer 2 logical interface configuration (units with encapsulation vlan-bridge configuration) is used, then the logical interface must be added as part of a bridge-domain or EVPN routing instance for the commit to succeed.

Network Management and Monitoring

- **NETCONF <kill-session> operation returns different values in <rpc-error> when the session identifier is equal to the current session ID (EX Series)**—Starting in Junos OS Release 19.1R1, when you execute the <kill-session> NETCONF operation and the session identifier is equal to the current session ID, the values of the <error-type> and <error-tag> elements in the resulting <rpc-error> are **application** and **invalid-value**, respectively. In earlier releases, the <error-type> and <error-tag> values are **protocol** and **operation-failed**.

[See [<kill-session>](#).]

Security

- **Syslog or log action on firewall drops packets (EX4600 switches)**—Starting in Junos OS Release 19.1R1, if you configure a syslog or log action on an ingress firewall filter, control packets and ICMP packets sent to the Routing Engine might be dropped.

User Interface and Configuration

- **Options for monitor traffic interfaces statement added (EX Series)**—Starting in Junos OS Release 19.1R1, the options **write-file** and **read-file** under the **monitor traffic** command are included in the visible CLI.

[See [monitor traffic](#).]

SEE ALSO

New and Changed Features	24
Known Behavior	32
Known Issues	33
Resolved Issues	37
Documentation Updates	41
Migration, Upgrade, and Downgrade Instructions	42
Product Compatibility	43

Known Behavior

IN THIS SECTION

- General Routing | 32
- Virtual Chassis | 33

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 19.1R1 for the EX Series.

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

General Routing

- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter will not be installed. [PR1362609](#)
- On EX4650 with 288,000 MAC scale, the Routing Engine **show ethernet-switching table summary** command output shows the learned scale entries after a delay of around 60 seconds. [PR1367538](#)
- Junos OS might hang trying to acquire the SMP IPI lock while rebooting when it is running as a VM on Linux and QEMU hypervisor. The device can be recovered using power-cycle of the device. [PR1385970](#)

Virtual Chassis

- A Virtual Chassis internal loop might happen at a node coming up from a reboot. During nonstop software upgrade (NSSU) on EX4600 and EX4300 Virtual Chassis, a minimal traffic disruption or traffic loop (greater than 2 seconds) might be seen. [PR1347902](#)

SEE ALSO

New and Changed Features	 24
Changes in Behavior and Syntax	 30
Known Issues	 33
Resolved Issues	 37
Documentation Updates	 41
Migration, Upgrade, and Downgrade Instructions	 42
Product Compatibility	 43

Known Issues

IN THIS SECTION

- [General Routing](#) | [34](#)
- [Infrastructure](#) | [35](#)
- [Interfaces and Chassis](#) | [35](#)
- [Junos Fusion Enterprise](#) | [35](#)
- [Layer 2 Features](#) | [36](#)
- [Multicast](#) | [36](#)
- [Network Management and Monitoring](#) | [36](#)
- [Platform and Infrastructure](#) | [36](#)
- [Routing Protocols](#) | [36](#)
- [Subscriber Access Management](#) | [37](#)

This section lists the known issues in hardware and software in Junos OS Release 19.1R1 for the EX Series.

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

General Routing

- Various common situations lead to different views of forwarding information between kernel and Packet Forwarding Engines. For example, **fpc7 KERNEL/PFE APP=NH OUT OF SYNC: error code 3 REASON: NH add received for an ifl that does not exist ERROR-SPECIFIC INFO: nh_id=562, type = Hold, ifl index 334 does not exist TYPE-SPECIFIC INFO: none**. No service impact is seen in MPC2 and MPC3 type line cards. [PR1205593](#)
- On an EX2300 switch, the output of the command **show chassis routing-engine** might display an incorrect value of "mac reset" for the "last reboot reason" field. [PR1331264](#)
- The change of authorization (CoA) messages are used to dynamically modify active subscriber sessions by using the CoA-ACK/CoA-NAK in response messages. After applying a multiterm IP filter by CoA, NAK might be received instead of ACK. When this happens, it might cause a change of authorization failure. [PR1361433](#)
- The time lapse between interface-down interrupt detection to FRR callback is approximately 148 ms on the EX4650 platform, though the in-place update FRR programming completes in 1 ms. The minimum FRR time achieved with this limitation is approximately 150 ms and maximum is approximately 275 ms. [PR1364244](#)
- When you swap a Virtual Chassis of QFX5100 to the EX9253 for testing some heavy multicast, even when the IRB interface comes up, traffic drop might be observed. [PR1369099](#)
- There are multiple failures when events such as node reboots, ICL flaps, and ICCP flaps occur; and even with **enhanced convergence** configured there is no guarantee that subsecond convergence will be achieved. [PR1371493](#)
- An EX4300 configured with a firewall filter on lo0 and DHCP-security on VLAN simultaneously might drop legitimate DHCP renew requests from clients on the corresponding VLANs. This occurs because of the implementation design and chipset limitation. [PR1376454](#)
- After the MACsec session is deleted, the corresponding interfaces might lose their MACsec function if LACP is enabled on them and the statement **exclude lacp** is configured under the **[security macsec]** hierarchy. [PR1378710](#)
- On EX9200 platforms, if a packet-length keyword under a firewall filter is applied on the interface egress, the configuration is not committed because of the commit-check failure. [PR1378901](#)
- When **show** command is takes long time to display results, the STP might change its' status as BPDUs are no longer processed and cause lots of outages. [PR1390330](#)
- DCPFE did not come up in some instances of abrupt power-off or power-on of EX4650. Power-cycle of the device or host reboot will recover the device. [PR1393554](#)
- Need 1-Gbps speed configuration support on EX9251. [PR1400651](#)

- After upgrading to Junos OS Release 18.1R3.3, the following output message is seen continuously: **adt7470_set_pwm**. [PR1401709](#)
- There is a possibility of seeing multiple reconnect logs, **JTASK_IO_CONNECT_FAILED**, during the device initialization. There is no functionality impact because of these messages. These messages can be ignored. [PR1408995](#)
- On EX9200 device with MCLAG configuration and other features enabled, there is a loss of approximately 20 seconds during restart of routing daemon. This traffic loss varies with the configuration that is done. [PR1409773](#)
- After back to back configuration change on EX4300-48MP, EVPN proxy ARP feature might no longer suppress ARP and/or network solicitation. However, IPv4 ARP and IPv6 network delivery (ND) process will still complete with remote destination host. [PR1414698](#)
- On EX4650 platforms, uRPF check in strict mode might not work appropriately. [PR1417546](#)
- Unable to access J-Web for switches EX2300 and EX3400. [PR1425205](#)

Infrastructure

- The logs were meant for VC packets which are flooded to internal HG-port to reach unit 0, and the physical interface in that case is NULL. [PR1381151](#)
- In a PVLAN multiple switches scenario, on EX2300, EX3400, EX4300, and EX4600 after rebooting the device, isolated VLAN traffic received from inter-switch link might be dropped. The configuration **inter-switch-link** statement is used when a private VLAN (PVLAN) spans multiple switches. [PR1388186](#)
- On EX2300/EX2300-C/EX2300-MP platforms, if Junos software is with FreeBSD kernel version 11 with the build date on or after 2019-02-12, the switch may stop forwarding traffic or responding to console. A reboot is required to restore the service. [PR1442376](#)

Interfaces and Chassis

- On GRES, VSTP port cost on aggregated Ethernet interfaces might get changed, leading to topology change. [PR1174213](#)

Junos Fusion Enterprise

- Power over Ethernet (PoE) over Link Layer Discovery Protocol (LLDP) negotiation is not supported in an Junos Fusion Enterprise setup. The issue results in powering up failure when a device makes PoE over LLDP negotiation with Junos Fusion Enterprise. [PR1366106](#)
- On Junos Fusion Enterprise setups, VOIP-enabled extended ports on satellite devices are set to the default MTU of 1514 bytes. Because of this, the maximum data size is limited to 1468 bytes, beyond which packets are dropped with MTU errors (when DF bit is set). [PR1411179](#)

Layer 2 Features

- On EX2300 and EX3400, if L2PT is configured and the user wants to enable LLDP, then the user needs to configure LLDP individually on the port. The **interface all** option does not work. There is no functional impact. [PR1361114](#)
- On EX2300 and EX3400, while configuring L2PT for tunneling LLDP, LLDP packets are dropped at the L2PT NNI interface. This issue is seen only the first time the configuration is done and recovers with reboot. [PR1362173](#)

Multicast

- IGMP query packets might be duplicated between Layer 2 interfaces with IGMP snooping enabled. [PR1391753](#)

Network Management and Monitoring

- In a rare case where trace files are not properly closed by the OS, trace option logs might stop writing to a log file. [PR1380764](#)

Platform and Infrastructure

- ICMPv6 packets are hitting the dynamic ingress filter with higher priority, thus never reaching an MF or static classifier. [PR1388324](#)

Routing Protocols

- If the gateway address is a MAC address, PIM is unable to process and crashes whenever a route uses qualified-next-hop. Hence, the gateway MAC address is set to null so that PIM can ignore it and continue with the regular processing as if there is no gateway address present. [PR1408443](#)
- EX4300-VC IGMP-Snooping might not work until multicast-snooping process is restarted. [PR1408443](#)

Subscriber Access Management

- The authd reuse address too quickly before jdhcpd completely cleanup the old subscriber which flooding error log . The log such as: `jdhcpd: %USER-3-DH_SVC_DUPLICATE_IPADDR_ERR: Failed to add 10.1.128.3 as it is already used by 1815.` [PR1402653](#)

SEE ALSO

New and Changed Features	 24
Changes in Behavior and Syntax	 30
Known Behavior	 32
Resolved Issues	 37
Documentation Updates	 41
Migration, Upgrade, and Downgrade Instructions	 42
Product Compatibility	 43

Resolved Issues

IN THIS SECTION

- [EVPN](#) | [38](#)
- [General Routing](#) | [38](#)
- [Infrastructure](#) | [39](#)
- [Junos Fusion Enterprise](#) | [39](#)
- [Layer 2 Features](#) | [40](#)
- [Layer 3 Features](#) | [40](#)
- [Platform and Infrastructure](#) | [40](#)
- [Routing Protocols](#) | [40](#)

This section lists the issues fixed in Junos OS Release 19.1R1 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.

EVPN

- A few minutes traffic loss might be observed during recovery from link failure. [PR1396597](#)

General Routing

- FPM board status is missing in SNMP MIB walk result. [PR1364246](#)
- The **OAM Ethernet connectivity-fault-management** configured on aggregated Ethernet interfaces is not supported; and no commit error is seen. [PR1367588](#)
- ARP request packets might be sent out with 802.1Q VLAN tag. [PR1379138](#)
- The 40-Gigabit Ethernet and 100- Gigabit Ethernet uplink port number options show incorrect number ranges. [PR1382578](#)
- Commit error is observed for the first time while loading the **mini-PDT base** configurations. [PR1383469](#)
- On the EX4650 switch, occasionally two of the channelized 25-Gigabit Ethernet ports that are using 4x25G breakout cable will not come up after Junos OS reboots. [PR1384898](#)
- ARP and ethernet-table entry in pointing to an aggregated Ethernet interface whose state is down. [PR1385199](#)
- On EX4300-48MP, the **session-option** stanza under the **[access profile]** hierarchy for EX Series and QFX Series platforms is not applicable. [PR1385229](#)
- On EX9200 platforms, the warning message **prefer-status-control-active** with **status-control standby** might be seen whenever you commit an operation. [PR1386479](#)
- On EX2300 with stacked VLAN, **flexible-vlan-tagging** is unable to obtain DHCP IP for IRB after a reboot/power-cycle. [PR1387039](#)
- On EX3400 Virtual Chassis, **Error tvp_status_led_set** and **Error:tvp_optics_diag_eeprom_read** syslog errors are seen. [PR1389407](#)
- MAC learning might stop working on some LAG interfaces. [PR1389411](#)
- On EX4300-48MP, need to remove messages **Recommend power cycle the device to complete the upgrade** and **Please power cycle the device to complete the upgrade** after ssd firmware upgrade. [PR1389543](#)
- "Input rate pps" is not increased on EX2300-MP uplink ports if the packet is a pure Layer 2 packet like non-etherII or non-EtherSnap. [PR1389908](#)
- The smid core file is generated during sanity script execution on QFX5100 and EX4300 switches. [PR1391909](#)
- PTP over Ethernet traffic might be dropped when IGMP and PTP TC are configured together. [PR1395186](#)
- DOT1XD core file is generated at **pnac_bd_create pnac_bdm_handler knl_async_receive_and_process**. [PR1395384](#)

- On EX2300, MAC table is not populated after interface-mode change. [PR1396422](#)
- High jsd or na-grpcd CPU usage might be seen even if JET or JTI is not used. [PR1398398](#)
- After upgrading Junos OS Release 15.1X53 to Junos OS Release 18.2R1.9, the EX3400 cannot learn 30,000 MAC addresses. [PR1399575](#)
- The FBF routing-instance instance-type "forwarding" is missed for EX Series (EX3400). [PR1400163](#)
- MAC-limit with persistent MAC is not working after reboot. [PR1400507](#)
- The authd might crash when you issue the **show network-access requests pending** command during authd restart. [PR1401249](#)
- On EX4300-48mp, packets are dropped after configuring traffic filter and routing instance. [PR1407424](#)
- The l2cpd might crash if the VSTP **traceoptions** and VSTP VLAN **all** commands are configured. [PR1407469](#)
- The chassisd output power budget is received continuously for 5 seconds without any alarm after upgrading to Junos OS Release 18.1R3. [PR1414267](#)
- VXLAN Encapsulation nexthop (VENH) does not get installed during BGP flap or restart routing. [PR1415450](#)

Infrastructure

- IfSpeed and IfHighSpeed are erroneously reported as zero on EX2300. [PR1326902](#)

Junos Fusion Enterprise

- An error **peer_daemon: bad daemon: scpd** is seen on EX9251 switch running Junos OS Releases 18.1R1 and 18.1R2. [PR1369646](#)
- Cannot login to SD cluster though it is recognized by AD properly. [PR1395570](#)
- The l2ald process might generate a core file when persistent MAC addresses are cleared from the switching table. [PR1409403](#)
- Extended ports do not adjust MTU in Junos Fusion Enterprise on VOIP-enabled ports. [PR1411179](#)

Layer 2 Features

- RTG MAC refresh packets are sent out from non-RTG ports if the RTG interface belonging to the Virtual Chassis master flaps. [PR1389695](#)

Layer 3 Features

- The l2ald might crash when the **clear ethernet-switching table persistent-learning** command is issued. [PR1381739](#)

Platform and Infrastructure

- Ping does not go through device after WTR timer expires in ERPS scenario. [PR1132770](#)
- EX4300 upgrade fails during validation of slax script. [PR1376750](#)
- ECMP route installation failure with log messages such as unilist install failure might be observed on EX4300 device. [PR1376804](#)
- Packet drops on interface if the statement **gether-options loopback** is configured. [PR1380746](#)
- Traffic loss is seen in Layer 2 VPN with GRE tunnel. [PR1381740](#)
- EX4300 device chooses incorrect bridge-id as RSTP bridge-id. [PR1383356](#)
- On EX4300-48MP switch mixed Virtual Chassis, PoE interface maximum power configuration on member EX4300 gives an error if configured more than 30. [PR1383717](#)
- Unicast DHCP request get misforwarded to backup RTG link on EX4300-VC. [PR1388211](#)
- ICMPV6 packets are not classified with static or multifield forwarding-class mapping. [PR1388324](#)
- Layer 3 IP route might be deleted after a Layer 2 next-hop change is seen. [PR1389688](#)
- Continuous log messages get printed in EX4300: **17.4 / MCSNOOPD ICCP Context./var/run/iccpd_control addr /var/run/iccpd_control: Connection refused.** [PR1391942](#)
- On EX4300 switches, tcpdump shows that the kernel is sending out the ARP response on receiving the ARP request, but that the response does not get on the wire. [PR1405168](#)
- The policer might not work when it is applied through the dynamic filter. [PR1410973](#)

Routing Protocols

- The PPM mode for BFD session in EX4300 is centralized and not distributed by default. [PR1361800](#)
- On EX4300-48MP, stale VLAN entries are seen after continuous script is run involving split, merge, and reboot. [PR1363739](#)

- On EX4650 switches, the command output for the **show pfe route summary hw** statement shows different scale values for the IPv4 and IPv6 LPM routes rather than the supported scale. [PR1366579](#)
- Host-destined packets with filter log action might reach the Routing Engine. [PR1379718](#)
- EX4300 might drop the incoming IS-IS hello packets when IGMP or MLD snooping is configured. [PR1400838](#)

SEE ALSO

New and Changed Features 24
Changes in Behavior and Syntax 30
Known Behavior 32
Known Issues 33
Documentation Updates 41
Migration, Upgrade, and Downgrade Instructions 42
Product Compatibility 43

Documentation Updates

There are no errata or changes in Junos OS Release 19.1R1 documentation for the EX Series switches.

SEE ALSO

New and Changed Features 24
Changes in Behavior and Syntax 30
Known Behavior 32
Known Issues 33
Resolved Issues 37
Migration, Upgrade, and Downgrade Instructions 42
Product Compatibility 43

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1, 17.2, and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

SEE ALSO

New and Changed Features 24
Changes in Behavior and Syntax 30
Known Behavior 32
Known Issues 33
Resolved Issues 37

Documentation Updates	41
Product Compatibility	43

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 43

Hardware Compatibility

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

To determine the features supported on EX Series switches in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://apps.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	24
Changes in Behavior and Syntax	30
Known Behavior	32
Known Issues	33
Resolved Issues	37
Documentation Updates	41
Migration, Upgrade, and Downgrade Instructions	42

Junos OS Release Notes for Junos Fusion Enterprise

IN THIS SECTION

- New and Changed Features | 44
- Changes in Behavior and Syntax | 45
- Known Behavior | 46
- Known Issues | 46
- Resolved Issues | 47
- Documentation Updates | 48
- Migration, Upgrade, and Downgrade Instructions | 48
- Product Compatibility | 54

These release notes accompany Junos OS Release 19.1R1 for Junos Fusion Enterprise. Junos Fusion Enterprise is a Junos Fusion that uses EX9200 switches in the aggregation device role. These release notes describe new and changed features, limitations, and known problems in the hardware and software.

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

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

New and Changed Features

IN THIS SECTION

- Junos Fusion Enterprise | 45

This section describes the new features and enhancements to existing features in Junos OS Release 19.1R1 for Junos Fusion Enterprise.

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

Junos Fusion Enterprise

- **Support for SFTP global disablement (Junos Fusion Enterprise)**—Starting in Junos OS Release 19.1R1, we have globally disabled incoming SSH File Transfer Protocol (SFTP) connections by default. You can enable incoming SFTP connections globally by configuring the statement **sftp-server** at the **[edit system services ssh]** hierarchy level. Prior to Junos OS Release 19.1R1, the incoming SFTP connections were globally enabled by default.

[See [Configuring sftp-server](#)]

SEE ALSO

Changes in Behavior and Syntax	45
Known Behavior	46
Known Issues	46
Resolved Issues	47
Documentation Updates	48
Migration, Upgrade, and Downgrade Instructions	48
Product Compatibility	54

Changes in Behavior and Syntax

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 19.1R1 for Junos Fusion Enterprise.

SEE ALSO

New and Changed Features	44
--	--------------------

Known Behavior	 46
Known Issues	 46
Resolved Issues	 47
Documentation Updates	 48
Migration, Upgrade, and Downgrade Instructions	 48
Product Compatibility	 54

Known Behavior

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 19.1R1 for Junos Fusion Enterprise.

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

SEE ALSO

New and Changed Features	 44
Changes in Behavior and Syntax	 45
Known Behavior	 46
Resolved Issues	 47
Documentation Updates	 48
Migration, Upgrade, and Downgrade Instructions	 48
Product Compatibility	 54

Known Issues

There are no known issues in hardware and software in Junos OS Release 19.1R1 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.

SEE ALSO

New and Changed Features	44
Changes in Behavior and Syntax	45
Known Behavior	46
Resolved Issues	47
Documentation Updates	48
Migration, Upgrade, and Downgrade Instructions	48
Product Compatibility	54

Resolved Issues

IN THIS SECTION

- Junos Fusion Enterprise | 47

This section lists the issues fixed in Junos OS Release 19.1R1.

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

- PoE over LLDP negotiation is not supported on Junos Fusion Enterprise setup. [PR1366106](#)
- An error **peer_daemon: bad daemon: scpd** is seen on EX9251 switch running Junos OS Releases 18.1R1 and 18.1R2. [PR1369646](#)
- Cannot login to SD cluster though it is recognized by AD properly. [PR1395570](#)
- The l2ald process might generate a core file when persistent MAC addresses are cleared from the switching table. [PR1409403](#)
- Extended ports do not adjust MTU in Junos Fusion Enterprise on VOIP-enabled ports. [PR1411179](#)

SEE ALSO

New and Changed Features	44
Changes in Behavior and Syntax	45

[Known Behavior | 46](#)

[Known Issues | 46](#)

[Documentation Updates | 48](#)

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

[Product Compatibility | 54](#)

Documentation Updates

There are no errata or changes in Junos OS Release 19.1R1 for documentation for Junos Fusion Enterprise.

SEE ALSO

[New and Changed Features | 44](#)

[Changes in Behavior and Syntax | 45](#)

[Known Behavior | 46](#)

[Known Issues | 46](#)

[Resolved Issues | 47](#)

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

[Product Compatibility | 54](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading Junos OS on an Aggregation Device | 49](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 51](#)
- [Preparing the Switch for Satellite Device Conversion | 51](#)
- [Converting a Satellite Device to a Standalone Switch | 52](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 53](#)
- [Downgrading from Junos OS | 53](#)

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:

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

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

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

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

```
user@host> request system software add validate reboot  
source/junos-install-ex92xx-x86-64-18.3B1.n.tgz
```

All other customers, use the following commands, where *n* is the spin number.

```
user@host> request system software add validate reboot  
source/junos-install-ex92xx-x86-64-18.3B1.n-limited.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

Preparing the Switch for Satellite Device Conversion

There are multiple methods to upgrade or downgrade satellite software in your Junos Fusion 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 switch running Junos OS can be converted only to SNOS 3.1 and later.
- Either the switch must be set to factory-default configuration by using the **request system zeroize** command, or the following command must be included in the configuration: **set chassis auto-satellite-conversion**.

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

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

2. Clear the device:

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Switch

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove it from the Junos Fusion topology. For more information, see [Converting a Satellite Device to a Standalone Device](#).

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1, 17.2, and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

Downgrading from Junos OS

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

NOTE: You cannot downgrade more than three releases.

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

To downgrade a Junos Fusion Enterprise from Junos OS Release 18.3R1, follow the procedure for upgrading, but replace the 18.3 **junos-install** package with one that corresponds to the appropriate release.

SEE ALSO

[New and Changed Features | 44](#)

[Changes in Behavior and Syntax | 45](#)

[Known Behavior | 46](#)

[Known Issues | 46](#)

[Resolved Issues | 47](#)

[Documentation Updates | 48](#)

Product Compatibility

IN THIS SECTION

- [Hardware and Software Compatibility | 54](#)
- [Hardware Compatibility Tool | 54](#)

Hardware and Software Compatibility

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

To determine the features supported in a Junos Fusion, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://apps.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 44
Changes in Behavior and Syntax 45
Known Behavior 46
Known Issues 46
Resolved Issues 47
Documentation Updates 48
Migration, Upgrade, and Downgrade Instructions 48

Junos OS Release Notes for Junos Fusion Provider Edge

IN THIS SECTION

- New and Changed Features | 55
- Changes in Behavior and Syntax | 56
- Known Behavior | 57
- Known Issues | 57
- Resolved Issues | 58
- Documentation Updates | 59
- Migration, Upgrade, and Downgrade Instructions | 59
- Product Compatibility | 68

These release notes accompany Junos OS Release 19.1R1 for the Junos Fusion Provider Edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- Authentication, Authorization and Accounting (AAA) (RADIUS) | 56

This section describes the new features and enhancements to existing features in Junos OS Release 19.1R1 for Junos Fusion Provider Edge.

Authentication, Authorization and Accounting (AAA) (RADIUS)

- **Support for SFTP global disablement (Junos Fusion Provider Edge)**—Starting in Junos OS Release 19.1R1, we have globally disabled incoming SSH File Transfer Protocol (SFTP) connections by default. You can enable incoming SFTP connections globally by configuring the statement **sftp-server** at the **[edit system services ssh]** hierarchy level. Prior to Junos OS Release 19.1R1, the incoming SFTP connections were globally enabled by default.

[See [Configuring sftp-server](#)]

SEE ALSO

Changes in Behavior and Syntax 56
Known Behavior 57
Known Issues 57
Resolved Issues 58
Documentation Updates 59
Migration, Upgrade, and Downgrade Instructions 59
Product Compatibility 68

Changes in Behavior and Syntax

There are no changes in default behavior and syntax for Junos Fusion Provider Edge in Junos OS Release 19.1R1.

SEE ALSO

New and Changed Features 55
Known Behavior 57
Known Issues 57
Resolved Issues 58
Documentation Updates 59
Migration, Upgrade, and Downgrade Instructions 59
Product Compatibility 68

Known Behavior

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 19.1R1 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	55
Changes in Behavior and Syntax	56
Known Issues	57
Resolved Issues	58
Documentation Updates	59
Migration, Upgrade, and Downgrade Instructions	59
Product Compatibility	68

Known Issues

There are no known issues in the Junos OS Release 19.1R1 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	55
Changes in Behavior and Syntax	56
Known Behavior	57
Resolved Issues	58
Documentation Updates	59
Migration, Upgrade, and Downgrade Instructions	59
Product Compatibility	68

Resolved Issues

IN THIS SECTION

- [Junos Fusion Provider Edge | 58](#)
- [Junos Fusion Satellite Software | 58](#)

This section lists the issues fixed in the Junos OS Release 19.1R1 for Junos Fusion Provider Edge.

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

Junos Fusion Provider Edge

- Broadcast, Unknown Unicast and Multicast(BUM) traffic might get dropped on peer Fusion Aggregation Device when link between Satellite Device and local Aggregate Device goes down. [PR1384440](#)

Junos Fusion Satellite Software

- Extended Port (EP) LAG might go down on the Satellite Devices (SDs) if the related Cascade Port (CP) links to an Aggregation Device (AD) goes down. [PR1397992](#)

SEE ALSO

- [New and Changed Features | 55](#)
- [Changes in Behavior and Syntax | 56](#)
- [Known Behavior | 57](#)
- [Known Issues | 57](#)
- [Documentation Updates | 59](#)
- [Migration, Upgrade, and Downgrade Instructions | 59](#)
- [Product Compatibility | 68](#)

Documentation Updates

There are no errata or changes in Junos OS Release 19.1R1 documentation for Junos Fusion Provider Edge.

SEE ALSO

New and Changed Features	 55
Changes in Behavior and Syntax	 56
Known Behavior	 57
Known Issues	 57
Resolved Issues	 58
Migration, Upgrade, and Downgrade Instructions	 59
Product Compatibility	 68

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading an Aggregation Device](#) | 60
- [Upgrading an Aggregation Device with Redundant Routing Engines](#) | 62
- [Preparing the Switch for Satellite Device Conversion](#) | 63
- [Converting a Satellite Device to a Standalone Device](#) | 64
- [Upgrading an Aggregation Device](#) | 66
- [Upgrade and Downgrade Support Policy for Junos OS Releases](#) | 67
- [Downgrading from Junos OS Release 19.1](#) | 67

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 [Installation and Upgrade Guide](#).

The download and installation process for Junos OS Release 19.1R1 is different from that for earlier Junos OS releases.

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

8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **jinstall** package on the aggregation device.

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

Customers in the United States and Canada, use the following commands.

- For 64-bit software:

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

```
user@host> request system software add validate reboot
source/jinstall64-19.1R1.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot
source/jinstall-19.1R1.SPIN-domestic-signed.tgz
```

All other customers, use the following commands.

- For 64-bit software:

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

```
user@host> request system software add validate reboot
source/jinstall64-19.1R1.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot
source/jinstall-19.1R1.SPIN-export-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 19.1R1 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

Preparing the Switch for Satellite Device Conversion

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

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

- The switch can be converted to only SNOS 3.1 and later.
- Either the switch must be set to factory-default configuration by using the **request system zeroize** command, or the following command must be included in the configuration: **set chassis auto-satellite-conversion**.

Customers with EX4300 switches, use the following command:

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

Customers with QFX5100 switches, use the following command:

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

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

1. Log in to the device by using the console port.
2. Clear the device:

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Device

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove the satellite device from the Junos Fusion topology.

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

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

1. Using a Web browser, navigate to the Junos OS software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads>
2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology > Junos Platform > Junos Fusion** from the drop-down list and select the switch platform series and model for your satellite device.
4. Select the Junos OS Release 14.1X53-D30 software image for your platform.
5. Review and accept the End User License Agreement.
6. Download the software to a local host.
7. Copy the software to the routing platform or to your internal software distribution site.
8. Remove the satellite device from the automatic satellite conversion configuration.

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

[edit]

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

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

[edit]

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

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

9. Commit the configuration.

To commit the configuration to both Routing Engines:

[edit]

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

Otherwise, commit the configuration to a single Routing Engine:

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

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

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

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

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

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

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

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

11. Wait for the reboot that accompanies the software installation to complete.
12. When you are prompted to log back into your device, 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 19.1R1, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1, 17.2, and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

Downgrading from Junos OS Release 19.1

To downgrade from Release 19.1 to another supported release, follow the procedure for upgrading, but replace the 19.1 **jinstall** package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

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

SEE ALSO

New and Changed Features 55
Changes in Behavior and Syntax 56
Known Behavior 57
Known Issues 57
Resolved Issues 58
Documentation Updates 59
Product Compatibility 68

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 68](#)

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 55
Changes in Behavior and Syntax 56
Known Behavior 57
Known Issues 57
Resolved Issues 58
Documentation Updates 59
Migration, Upgrade, and Downgrade Instructions 59

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

IN THIS SECTION

- New and Changed Features | 69
- Changes in Behavior and Syntax | 90
- Known Behavior | 96
- Known Issues | 99
- Resolved Issues | 110
- Documentation Updates | 123
- Migration, Upgrade, and Downgrade Instructions | 123
- Product Compatibility | 130

These release notes accompany Junos OS Release 19.1R1 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- Release 19.1R1-S1 New and Changed Features | 70
- Release 19.1R1 New and Changed Features | 70

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

Release 19.1R1-S1 New and Changed Features

Interfaces and Chassis

- **MPC10 Distributed LACP Support in PPM AFT (MX Series)**—Starting in Junos OS Release 19.1R1S1 and 19.1R2, MPC10E-15C-MRATE and MPC10E-10C-MRATE MPCs support distributed LACP in Periodic Packet Manager (ppman) Advanced Forwarding Toolkit (AFT).

Routing Protocols

- **MPC10 Inline BFD support (MX Series)**—Starting in Junos OS Release 19.1R2, MPC10 MPCs support inline BFD features, excluding micro BFD and BFD sessions with authentication.

[See [Understanding BFD for Static Routes](#).]

Release 19.1R1 New and Changed Features

Hardware

- **New Fixed-Configuration Modular Port Concentrator (MX240, MX480, and MX960)**—Starting in Junos OS Release 19.1R1, the MPC10E-15C-MRATE is a new Modular Port Concentrator (MPC) that is supported on MX240, MX480, and MX960 routers.

The MPC10E-15C-MRATE features the following:

- Line-rate throughput of up to 1.5 Tbps.
- Twelve QSFP28 ports—Port numbers 0/0 through 0/3, 1/0 through 1/3, and 2/0 through 2/3. The ports can be configured as 10-Gbps, 40-Gbps, or 100-Gbps Ethernet ports.
- Three QSFP56-DD ports—Port numbers 0/4, 1/4, and 2/4. The ports can be configured as 10-Gbps, 40-Gbps, 100-Gbps Ethernet ports.

See [MX Series 5G Universal Routing Platform Interface Module Reference](#).

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

- **Support for SFTP global disablement (MX Series)**—Starting in Junos OS Release 19.1R1, we have globally disabled incoming SSH File Transfer Protocol (SFTP) connections by default. You can enable incoming SFTP connections globally by configuring the statement **sftp-server** at the **[edit system services ssh]** hierarchy level. Prior to Junos OS Release 19.1R1, the incoming SFTP connections were globally enabled by default.

[See [Configuring sftp-server](#).]

Class of Service (CoS)

- **Support for CoS features (classifiers, rewrites, port queuing, L3 interfaces only) (MX Series)**—Starting with Junos OS Release 19.1R1, you can configure the standard CoS forwarding (classifiers, rewrites, port queuing, L3 interfaces only) on MPC10E line cards.

[See [Understanding Class of Service](#)]

- **Support for Real-time Transport Protocol (RTP) payload types 96 through 127 on inline video monitoring (MX Series)**—Starting with Junos OS 19.1, you can configure MX Series Routers for inline video monitoring of uncompressed HD or 4K stream video (Payload Type 96 through 127). MDI functionality has been extended to video flows such as ST 2000-5 (RTP PT 98) and ST 2000-6 (RTP PT 99). These are non-MPEG video flows over IP/UDP/RTP and are constant bit rate flows. The operator would specify proper IP addresses and UDP ports so that non-video flows over RTP will not go through MDI processing.

[See [Understanding Inline Video Monitoring on MX Series Routers](#)]

EVPN

- **Support for auto-derived route target on EVPN-MPLS (MX Series)**—Starting in Junos OS Release 19.1R1, Junos OS supports the automatic derivation of a route target on EVPN-MPLS. With this feature, the route target is automatically derived from the VLAN ID for EVPN type 2 and EVPN type 3 routes. The auto-derived route targets have higher precedence over manually configured RT in vrf-target, vrf-export policies, and vrf-import policies.

To enable auto-derived route target, include the **auto** statement at the **[edit routing-instances routing-instance-name protocols evpn vrf-target]** hierarchy level.

[See [Auto-derived Route Targets.](#)]

- **Support for proxy MAC addresses in an ARP request (MX Series)**—Starting in Junos OS Release 19.1R1, provider edge (PE) devices in an EVPN network that support ARP proxy can use a proxy MAC address in the ARP replies message to a host. When a PE device receives an ARP request or NDP request, it searches its MAC-IP address binding database for the requested IP address. If the device finds the MAC-IP address entry in its database, it responds to the request with the proxy MAC address. The proxy MAC address is derived from the IRB interface in an EVPN network with edge-routed bridging overlay and from the manually configured MAC address in a centrally-routed bridging overlay. If the device does not find an entry, the PE device replaces the MAC and IP address from the CE device in the ARP request with the proxy MAC and IP address of the IRB interface. This allows for enhanced security (i.e. L3 filtering) deployments on L3 gateway for both inter-VLAN and intra-VLAN traffic will be routed.

To enable this feature, configure the **proxy-mac [irb | proxy-mac-address]** statement at the **[edit routing-instances routing-instance-name protocols evpn]** hierarchy or at the **[edit routing-instances routing-instance-name bridge-domains domain_name]** hierarchy.

[See [ARP and NDP Request with a proxy MAC address.](#)]

- **Support for asynchronous notification on EVPN-VPWS (MX Series)**—Starting in Junos OS Release 19.1R1, asynchronous-notification is supported on interfaces on EVPN-VPWS. You can enable the asynchronous notification command to send a loss of signal (LOS) alarm to the CE device when the circuit cross-connect link between a customer edge and provider edge device goes down. Asynchronous notification supports ethernet-ccc, ethernet-vpls, or vlan-ccc encapsulation.

To enable this feature, include the **asynchronous-notification** statement at the **[edit interfaces interface-name]** hierarchy level.

[See [Configuring Gigabit Ethernet Notification of Link Down Alarm](#).]

Forwarding and Sampling

- **Support for tracking static RPM routes across multiple next hops (MX Series)**—Starting in Junos OS Release 19.1R1, you can use **rpm-tracking** to track up to 16 next hops for RPM-controlled static routes. This feature supports both IPv4 and IPv6 static rpm-tracked routes, and extends the single hop **rpm-tracking** introduced in Junos OS Release 18.4.

[See [show route rpm-tracking](#).]

- **Support for using IP addresses in an SR-TE LSP segment list (MX Series)**—Starting in Junos OS Release 19.1R1, you can use IP addresses (IPv4 or IPv6) for next hops in a segment routing traffic engineering (SR-TE) list of label-switched paths (LSPs). This work extends the support for traffic steering based on a segment routing policy that was introduced in Junos OS Release 17.4R1, wherein the controller can specify a segment routing policy consisting of multiple paths to steer labeled or IP traffic.

[See **auto-translate** in [segment-list](#) and **retry-timer** in [source-packet-routing](#) .]

Interfaces and Chassis

- **Support for MPC10E-15C-MRATE line card on MX240, MX480, MX960**—Starting with Junos OS Release 19.1R1, the MX240, MX480 and MX960 routers support the MPC10E-15C-MRATE (15x100GE) line card. This fixed-port line card is capable of delivering a bandwidth of up to 1.5 Tbps per MPC slot. It supports three MICs (one per Packet Forwarding Engine), each of which can deliver a throughput of up to 500 Gbps. Each MIC comprises five ports that support 100 Gbps (the default), 40 Gbps, and 10 Gbps speeds through the use of QSFP28+ and QSFP+ optics. You enable 10 Gbps speed (four 10 Gbps channels) by using breakout cables.

NOTE:

- The MPC10E-15C-MRATE is powered on only if the MX Series router has an enhanced Switch Control Board (MX-SCBE3) installed.
- The MPC10E-15C-MRATE is supported only with the high-capacity AC and DC power entry modules (PEMs) and the high-capacity fan trays used in MX Series routers.
- The MPC10E-15C-MRATE is powered on only if the router operates in **enhanced-ip** or **enhanced-ethernet** mode.
- The MPC10E-15C-MRATE is not supported on the MX2000 and MX10000 lines of routers.

[See [MPC10E-15C-MRATE](#), [Understanding Interface Naming Conventions for MPC10E-15C-MRATE MPC](#), [MPC10E-15C-MRATE Rate-Selectability Overview](#), [Supported Active Physical Ports for Rate Selectability to Prevent Oversubscription on MPC10E-15C-MRATE](#), and [Configuring Rate Selectability on MPC10E-15C-MRATE to Enable Different Port Speeds](#).]

- **Chassis and power management for MPC10E-15C-MRATE (MX240, MX480, and MX960)**—Starting in Junos OS Release 19.1R1, the MX240, MX480, and MX960 routers with the MPC10E-15C-MRATE line

card support chassis management features, including field replaceable unit (FRU) management, power budgeting and management, and environmental monitoring. The MPC10E-15C-MRATE line card supports configuration of ambient temperature (25°C, 40°C, and 55°C) and dynamic power management. The default ambient temperature value supported is 40°C. The MPC10E-15C-MRATE line card supports both hyper mode (the default mode) and normal mode.

NOTE:

- The MPC10E-15C-MRATE is powered on only if the MX Series router has an enhanced Switch Control Board (MX-SCBE3) installed.
- The MPC10E-15C-MRATE is powered on only if the router operates in **enhanced-ip** or **enhanced-ethernet** mode.
- The MPC10E-15C-MRATE will be powered on only when the MX Series router is installed with enhanced Fan Trays.
- The MPC10E-15C-MRATE will be supported only when the MX Series router is installed with Enhanced PEMs.
- On MX960 routers with enhanced Midplane on the slot 1, the MPC10E-15C-MRATE will not be powered on.

[See [Understanding How Configuring Ambient Temperature Helps Optimize Power Utilization](#) and [Understanding How Dynamic Power Management Enables Better Utilization of Power](#).]

- **PFE power on and power off support for MPC10E-15C-MRATE (MX240, MX480, and MX960)**—Starting Junos OS Release 19.1R1, on MX240, MX480, and MX960 devices with MPC10E-15C support, you can power on or power off a Packet Forwarding Engine using the command **set chassis fpc slot-number pfe slot-number power (on | off)**.

The **show chassis fpc FPC Slot detail** displays the PFE power ON/OFF status and bandwidth for the individual PFEs in an MPC10E-15C-MRATE.

See [show chassis fpc](#).

- **Support for ETH-ED (MX Series)**—Starting with Junos OS Release 19.1R1, when a unified in-service software upgrade (unified ISSU) is about to start, the peer maintenance association end point (MEP) is notified to suppress the remote defect indication (RDI) and loss of adjacency alarms for a specified duration. To ensure that the notification is sent before the upgrade starts, you must configure the Ethernet expected defect (ETH-ED) function by including, **expected-defect** statement at the **[edit protocols oam ethernet connectivity-fault-management expected-defect]** hierarchy level.

[See [connectivity-fault-management](#).]

- **Support for inline LACP PDU transmission processing (MX Series routers with MPCs)**—Starting in Junos OS Release 19.1R1, MX Series routers with MPCs support inline LACP PDU transmission processing for periodic packet management (on the Packet Forwarding Engine). To enable the inline processing method

instead of using the default LACP PDU transmission processing, issue the **set protocols lacp ppm inline** command.

[See [inline](#).]

- **Improved performance of small packets (MX Series)**—Starting in Junos OS Release 19.1R1, the MPC7E-MRATE, MPC7E-10G, MPC8E, MPC9E, MX10003 MPC, MX204, and JNP10K-LC2101 line cards provide improved performance of small packets (with a minimum packet size of 64 bytes) in transmit direction. To enable this feature, reduce the number of active ports (at the PIC level) to the following maximum numbers:
 - Sixteen 10-Gbps ports
 - Four 40-Gbps ports
 - Two 100-Gbps ports (when the line card is in 240-Gbps mode)
 - Three 100-Gbps ports (when the line card is in 400-Gbps mode)

To configure the number of active ports, use the existing command **set chassis fpc slot pic slot number-of-ports number-of-active-ports**.

NOTE:

- The command does not change packet performance at the Packet Forwarding Engine level; it improves packet performance in transmit direction at the port level only.
- For an MX10003 MPC, in 40-Gbps and 10-Gbps PIC modes, if both the PICs are used, the number of ports cannot exceed six on either PIC. If only PIC 1 is used, you can set the number of ports to 12. For an MX204 MPC, in 10-Gbps PIC mode, if both the PICs are used, the sum of the interfaces created on the PICs cannot exceed 16. If only PIC 0 is used, you can set the number of ports to 4 (4 interfaces per port). If only PIC 1 is used, you can set the number of ports to 8 (1 interface per port).

See [Understanding Rate Selectability](#)

IPsec

- **Distinguished name support in IPsec (MX Series)**—Starting with Junos OS Release 19.1R1, distinguished name support (DN) is added to the IKE identification (IKE ID) that is used for validation of VPN peer devices during IKE negotiation. The IKE ID received by an MX Series router from a remote peer can be an IPv4 or an IPv6 address, a hostname, a fully qualified domain name (FQDN), or a distinguished name (DN). The IKE ID sent by the remote peer needs to match what is expected by the MX Series router. Otherwise, IKE ID validation fails and the VPN is not established.

A distinguished name (DN) is a name used with digital certificates to uniquely identify a user. You can use a container keyword to specify the order of the fields in a distinguished name and their values must exactly match the configured distinguished name, or use a wildcard keyword to specify that the values of fields must match but the order of the fields does not matter.

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

- **Support for IPsec and Group VPN services on MX2010 and MX2020 routers (MX Series)**—Starting in Junos OS Release 19.1R1, Junos OS supports IPsec and Group VPN services on MX2010 and MX2020 routers. Group VPNs eliminate the need for point-to-point VPN tunnels in a mesh architecture. It is a set of features that are necessary to secure unicast traffic over a private WAN that originates on or flows through a router.

[See [Group VPNv2 Overview](#)]

Junos Telemetry Interface

- **RSVP interface OpenConfig model support and self-ping logs on Junos Telemetry Interface (JTI) (MX960 and PTX10003)**—Starting in Junos OS Release 19.1R1, JTI sensor support is enhanced for RSVP interfaces to include delivery of more statistics. The level of support is equivalent to the output delivered when using the **show rsvp interface detail** operational mode command.

To configure the sensor for statistics to be issued to an outside collector, include the following path for gRPC streaming:

- `/network-instances/network-instance/mpls/signaling-protocols/rsvp-te/interface-attributes/interfaces/interface/*`

To provision the sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support the Junos Telemetry Interface (JTI).

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

- **Delegated RPM statistics sensor support for Junos Telemetry Interface (JTI) (MX Series)**—Starting with Junos OS Release 19.1R1, for MX Series routers operating with MS-MIC and MS-MPC, a new sensor allows customers to monitor delegated RPM service statistics on the router and export them to outside collectors at configurable intervals encoded in Google Protocol Buffer (GPB) format.

Delegated RPM is a mode where RPM probe generation and measurement calculation are done by MS-MIC and MS-MPC cards. This hardware assistance allows a very high scale of concurrent RPM probes. JTI sensor support for other RPM modes was added in Junos OS Release 18.3R1.

You can use the resulting data from this sensor to improve network design and optimize traffic engineering. Data can also be used to detect problems in individual devices as well as in the overall network and the traffic carried by it.

Monitor delegated RPM service statistics by configuring the `/junos/services/spu/delegated-rpm/` sensor for the **sensor** configuration statement.

For exporting statistics, configure parameters at the **[edit services analytics]** hierarchy level.

[See [sensor \(Junos Telemetry Interface\)](#) and [Configuring a Junos Telemetry Interface Sensor \(CLI Procedure\)](#) and [Junos OS Release Notes for MX Series 5G Universal Routing Platform, 18.3R1](#).]

- **Export of data associated with the Junos kernel through Junos Telemetry Interface (JTI) (EX9200, EX9251, EX9253, MX Series, and PTX Series)**—Starting in Junos OS Release 19.1R1, you can export data associated with the Junos kernel through remote procedure calls (gRPC) and JTI. Kernel telemetry data includes information on Veriexec state, graceful Routing Engine switchover (GRES), in-service software upgrade (ISSU), and Routing Engine ifstate. Junos kernel sensors can be used by device monitoring and network analytics applications to provide insight into the health status of the Junos kernel.

Junos kernel sensors introduced in Junos OS Release 19.1R1 support both periodical and ON_CHANGE streaming. The following Junos kernel resource paths support periodical streaming only:

- /junos/kernel-ifstate/dead-ifstates-cnt
- /junos/kernel-ifstate/alive-ifstates-cnt
- /junos/kernel-ifstate/delayed-unrefs-cnt
- /junos/kernel-ifstate/delayed-unrefs-max

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

- **SRTE Telemetry statistics and BINDING-SID routes support for uncolored SRTE policies (MX Series)**—Starting in Release 19.1R1, Junos OS supports SRTE telemetry statistics and BINDING-SID routes for uncolored SRTE policies. Uncolored SRTE LSP is characterized by the absence of **color** statement in its configuration.

Junos OS now allows collection of traffic statistics for both ingress IP traffic and transit MPLS traffic that take uncolored SRTE paths. Also, you can install BINDING-SID labels even if the first hop of the segment list is a label. Prior to Junos OS 19.1R1 Release, the installation of BSID routes was not supported if the first hop of the segment list was a label, and a commit check was done.

The **show spring-traffic-engineering lsp** command is enhanced to provide the source by which the SRTE policy was provisioned. For example, Static, Path Computation Element Protocol. Also, the **show spring-traffic-engineering lsp detail** command is enhanced to provide information on the source of the tunnel configuration and statistics.

By default, traffic sensors and statistic collection are disabled for static SRTE routes. To enable provisioning of JVISION traffic sensors in Junos OS data plane to stream out traffic statistics on SR policies and their Binding-SID routes, use the existing **statistics** statement at the **[edit source-packet-routing telemetry]** hierarchy level.

Layer 3

- **Support for Layer 3 features on the MPC10E line card (MX Series)**—Starting in Junos OS Release 19.1R1, Junos OS supports the following Layer 3 features on the MPC10E line card.
 - BGP (multipath/v4-v6 labelled unicast)
 - IPv4 (forwarding and options)

- IPv6 (forwarding and route accounting)

- Load balancing (ECMP and FRR)

Options supported: enhanced -hash-key family inet/inet6/mpls

- L2VPN, CCC, and L2 Circuit

- MPLS (Push/Pop/Swap, LDP, RSVP-Aggregate, RSVP TE Admin Groups, RSVP-TE, OAM - LSP/VPN ping, Trace Route, Auto Bandwidth, and MPLS-FRR Link node protection.

Options supported: No Decrement Ttl, No Propagate Ttl, MTU-signaling Splitting-merging, Primary/Secondary, ICMP Tunneling, IPv6 Tunneling, LDP Tunneling, Optimize Timer, Explicit-Null, UHP and PHP support.

- OSPF (node-link-protection and node-link-degradation)
- Protocols (ISIS, OSPF, OSPF V3 for V6, BGP + BGP-v6, BGP LU, BGP-LS, BGP optimal-route-reflection (ORR), BFD (Centralized), Micro BFD(Centralized), ICMP and ICMPv6 error handling, and LLDP).
- Routing Instance Logical System VRF
- Tunnel (Generic Routing Encapsulation (GRE), Logical Tunnel (LT), and Virtual Tunnel (VT))

[See [Tunnel Services Overview](#)]

Management

- **Tracing support for individual JET application files (MX Series)**—Previously you could configure traceoptions for all applications. Starting in Junos OS Release 19.1R1, you can also configure traceoptions for an individual application file. If you configure trace options both globally (all applications) and locally (by application file), the local configuration has the higher priority. You must commit global traceoptions and the daemonized application configurations at the same time for the global traceoptions for the daemonized application to take effect.

[See [application](#).]

MPLS

- **Flexible MPLS label stack depth (MX Series with MPC and MIC)**—Currently, Junos OS supports push of up to a maximum of 5 labels per component of the next hop chain, even though the underlying device capability can be higher. Starting in Junos OS Release 19.1R1, the device capability of pushing more than 5 labels can be leveraged for features, such as, segment routing traffic-engineering (TE) LSPs and RSVP-TE pop-and-forward LSPs.

The number of labels that can be pushed for an MPLS next hop is the number of labels the device is capable of pushing, or the maximum-labels configured under **family mpls** of the outgoing interface, whichever is smaller.

[See [Configuring the Maximum Number of MPLS Labels, maximum-labels](#).]

- **Support for MPLS ping and traceroute for segment routing (MX Series)**—Starting in Junos OS Release 19.1R1, MPLS ping and traceroute are supported for segment routing (SR) for protocols ISIS and OSPF over IPv4. This feature also supports ECMP traceroute for protocols ISIS and OSPF.

On MX Series, MPLS ping and traceroute for segment routing is supported with enhanced-ip mode only. Segment routing with ISIS tunnels are stitched to LDP tunnels. Ping and traceroute for segment routing over RSVP is supported.

In Junos OS Release 19.1R1, MPLS ping and traceroute for segment routing supports IPv4 IGP-Prefix segment FEC validation. FEC validation for IGP-Adjacency Segment ID is not supported.

[See [ping mpls segment routing isis](#), [ping mpls segment routing ospf](#), [traceroute mpls segment-routing ospf](#), [traceroute mpls segment-routing isis](#).]

- **Support for new MPC line card MPC10 (MX Series)**—Starting in Junos OS Release 19.1R1, a new MPC line card MPC10 is introduced.

The following MPLS features are supported on MPC10 in 19.1R1:

- Static, RSVP and LDP LSPs
- LSP statistics
- LSP ping and traceroute

- LSP TTL knobs: no-propagate-ttl, no-decrement-ttl
- L2Circuit and L2VPN with or without control word
- L3VPN with chain-composite-nexthop
- L3VPN with vrf-table-label
- MPLS link protection, node protection and FRR
- 6VPE

The following MPLS features are not supported on MPC10 in 19.1R1:

- VCCV BFD
- L2CKT/L2VPN interworking (iw interface)
- Translational Cross-Connect (TCC)
- Flow aware transport (FAT) label
- Entropy Label
- **Enhancements to MPLS for LSP path selection (MX Series)**—Starting in Junos OS Release 19.1R1, the following enhancements to MPLS have been added for LSP path selection and optimization:
 - Earlier when LSP active paths were modified, the LSP path gets cleared and gets resignalled immediately. From Junos OS Release 19.1R1 onwards, if a secondary path is available, then Junos OS selects the secondary path as active, clears and resignals the primary path after the expiry of the **optimize-hold-dead-delay** timer. When the primary LSP path is established, the **revert-timer** gets started. After the **revert-timer** expires, the primary LSP path becomes active.

If the primary LSP path is not active with **revert-timer** on and when there is a change to the primary LSP path, then the LSP path gets cleared and resignalled immediately. When the primary LSP path is established, the revert-timer gets restarted.
 - Earlier if there was any Constrained Shortest Path First (CSPF) failure then the current LSP path becomes invalid because it did not match with the configured constraints. In this case, the current LSP path gets cleared immediately. From Junos OS Release 19.1R1 onwards, if a secondary LSP path is available, then Junos OS selects the secondary LSP path as active and clears the primary path after the expiry of the **optimize-hold-dead-delay** timer.
 - The CLI knob **no-bypass-statistics-polling** added under the `[edit protocols mpls statistics]` hierarchy now provides information on bypass LSP statistics.
 - A new CLI knob **delay** has been introduced under the `[edit protocols mpls optimize-adaptive-teardown]` hierarchy and the value for delay is in the range of (3..65535 seconds). When the **adaptive-teardown** configuration is triggered, the **delay** CLI knob further delays the tearing down of old optimized LSP paths based on the configured value.

[See [statistics \(Protocols MPLS\)](#), [optimize-adaptive-teardown](#).]

- **Use of SID labels as first hop for resolving non-colored static segment routing LSPs (MX Series)**—Currently, for a static non-colored segment routing traffic-engineered LSP to be usable, the first hop of the segment list must be an IP address. Only the second to *n*th hop could be segment identifier (SID) labels. Starting in Junos OS Release 19.1R1, this requirement does not apply. You can now configure SID labels as the first hop in the segment list.

With this configuration, static non-colored segment routing LSPs are resolved using MPLS fast reroute (FRR) and weighted equal-cost multipath. Without this configuration, by default, the LSPs are resolved using IP address.

[See [Static Segment Routing Label Switched Path](#).]

- **Support of install statement for segment routing LSPs (MX Series)**—The `install destination-prefix` statement which is currently supported at the `[edit protocols mpls label-switched-path lsp-name]` and `[edit protocols mpls static-label-switched-path lsp-name ingress]` hierarchy levels is now also supported at the `[edit protocols source-packet-routing source-routing-path lsp-name]` hierarchy level for both colored and non-colored static segment routing label-switched paths (LSPs).

You can associate one or more prefixes with a segment routing LSP using the `install` statement. When the LSP is up, all the prefixes are installed as entries into the `inet.3` or `inet6.3` routing table.

[See [install \(Protocols MPLS\)](#).]

- **Control transport address used for targeted-LDP session (MX Series)**—Currently, only the router-ID or interface address is used as the LDP transport address. Starting in Junos OS Release 19.1R1, you can configure any other IP address as the transport address of targeted LDP sessions, session-groups, and interfaces. This new configuration is applicable only for configured LDP neighbors that have Layer 2 circuit, MPLS, and VPLS adjacencies.

This feature is beneficial when you have multiple loopback interface addresses, and different IGPs associated with LDP interfaces, and you can control the session established between targeted LDP neighbors with the configured transport address.

[See [Control Transport Address Used for Targeted-LDP Session](#).]

- **MPLS egress traffic statistics for label IS-IS routes at ingress device (MX Series with MPC and MIC)**—Currently, sensors are available for collecting segment routing statistics for MPLS transit traffic, which is MPLS-to-MPLS in nature. Starting in Junos OS Release 19.1R1, additional sensors are introduced to collect segment routing statistics for MPLS egress traffic at the ingress provider edge (PE) device, which is IP-to-MPLS in nature.

With this feature, you can enable sensors for label IS-IS segment routing egress traffic only, and stream the statistics to a gRPC client.

[See [Understanding Source Packet Routing in Networking \(SPRING\)](#).]

- **Policy-based multipath routes (MX Series)**—In segment routing networks with multiple protocols in the core, you can combine segment routing traffic-engineered (SR-TE) LDP routes and SR-TE IP routes to create a multipath route that is installed in the routing information base (also known as routing table).

You can resolve BGP service routes over the multipath route through policy configuration and steer traffic differently for different prefixes.

[See [Policy-Based Multipath Routes Overview](#).]

- **Support of Layer2 and Layer3 VPN services over non-colored Segment Routing for Traffic Engineering (SR TE) (MX Series)**— Starting from Junos OS Release 19.1R1, you can use BGP-based Layer2 and Layer3 VPN services over non-colored Segment Routing for Traffic Engineering (SR TE). You can also use other features such as un-balanced ECMP (wecmp), and multi-level weighted ECMP (h-wecmp).

To use hierarchical multi-level weighted ECMP (h-wecmp), configure the following route resolution import-policy:

```
set policy-options policy-statement mpath then multipath-resolve
set routing-options resolution rib bgp.l3vpn.0 inet-import mpath
set routing-options resolution rib bgp.l2vpn.0 inet-import mpath
set routing-options resolution rib mpls.0 inet-import mpath
```

[See [Static Segment Routing Label Switched Path](#)]

- **Routing Engine-based S-BFD for segment-routing traffic engineering (MX Series)**—Starting in Junos OS Release 19.1R1, you can run Routing Engine-based seamless BFD (S-BFD) over non-colored and colored label-switched paths (LSPs) with first-hop label resolution and use S-BFD as a fast mechanism to detect path failures.

[See [Routing Engine-based S-BFD for Segment-Routing Traffic Engineering with First-Hop Label Resolution](#).]

Multicast

- **Support for next-generation MVPN Inter-AS option B (T4000)**—Starting in Junos OS Release 19.1R1, for improved security and scalability, Juniper supports Rosen Inter-AS option B for next-generation multicast virtual private networks (MVPNs) and segmented provider tunnels. Only specific configurations are supported, so for example, static tunnels (such as RSVP-TE and IR) are not supported, nor are PIM any-source multicast (ASM) and PIM source-specific multicast (SSM) tunnels.

In the supported configuration, next-generation MVPN sites can span multiple autonomous system (AS) boundaries (that is, domains). Each AS can implement its own p-tunnel (they don't have to be the same). Per-VPN subinterfaces are not shared between ASBRs. Likewise, provider edge (PE) routers from one AS cannot be reached from another AS, and the AS topology of one site is not exposed to any others.

[See [inter-as \(Routing Instances\)](#) and [BGP-MVPN Inter-AS Option B Overview](#).]

- **Support for multicast forwarding on MPC10E-MRATE line cards (MX Series)**—Starting in Junos OS Release 19.1R1, multicast forwarding is fully supported on MPC10E-MRATE line cards for MX Series routers.

Network Management and Monitoring

- **Error handling and resiliency support for MPC10E (MX240, MX480, and MX960)**—Starting in Junos OS Release 19.1R1, the MX240, MX480, and MX960 routers with MPC10E (MPC10E-15C-MRATE) line cards support error handling and software resiliency. The MPC10E supports detecting errors, reporting them through alarms, and triggering resultant actions. Use the existing commands **show chassis errors active**, **show chassis errors active details**, and **show chassis fpc errors** to view more details of the errors. MPC10E-15C-MRATE also supports powering on or off Packet Forwarding Engine (pfe2), by using the command **set chassis fpc slot pfe slot power (on|off)**, in case of errors such as hardware components issues in Packet Forwarding Engine (pfe2).

[See [show chassis fpc errors](#) and [clear chassis fpc errors](#).]

- **sFlow performance improvements (MX Series)**—Starting in Junos OS Release 19.1R1, the following improvements have been added to the sFlow technology feature:
 - For MX Series, the maximum number of samples per second per line card is raised from 950 pps to 9500 pps. Junos OS also introduces an adaptive sampling fallback feature, which decreases the sampling load when the traffic load decreases after adaptive sampling has taken place.
 - For MX Series, PTX Series, and QFX Series, you can configure forwarding class and DSCP values per collector.
 - For MX Series, dual vlans are supported.
 - For MX Series, true output interface (OIF) is supported.
 - Enhancements are made to the following CLI commands: **show sflow collector**, **show sflow collector address ip-address**, and **show sflow interface**.

[See [Understanding How to Use sFlow Technology for Network Monitoring](#), [collector](#), [agent-id](#), [source-ip](#), [show flow collector](#), and [show flow interface](#).]

Routing Policy and Firewall Filters

- **Support for firewall forwarding on MPC10E-MRATE line cards (MX Series)**—Starting in Junos OS Release 19.1R1, firewall forwarding is fully supported on MPC10E-MRATE line cards for MX Series routers.

Routing Protocols

- **Support for BGP graceful shutdown (MX Series)**— Starting in Junos OS Release 19.1R1, graceful traffic migration from one BGP next hop to another is supported, without traffic interruption. Also, BGP administrative shutdown communication can be sent to the BGP peer.

You can configure both **graceful-shutdown** and **shutdown** statements at the `[edit protocols bgp]`, `[edit protocols bgp group group-name]`, and `[edit protocols bgp group group-name neighbor address]` hierarchy levels.

NOTE: Graceful shutdown is disabled by default.

[See: [graceful-shutdown \(Protocols BGP\)](#), [shutdown \(Protocols BGP\)](#).]

- **Support for anycast and prefix segments in SPRING for OSPF protocols (MX Series)**—Starting in Junos OS Release 19.1R1, anycast and prefix segments are supported in SPRING. An anycast segment enforces forwarding based on the equal-cost multipath-aware shortest-path toward the closest node of the anycast set. Within an anycast group, all the routers advertise the same prefix with the same SID value, which facilitates load balancing. You can designate prefix segment indexes to prefix SIDs, both anycast and node SIDs, that are advertised in OSPF through policy configuration. Remote routers use this index to consolidate prefixes into respective SRGBs and to derive the segment identifier and forward the traffic destined for a specific prefix.

You can also configure **explicit-NULL** flag on all prefix SID advertisements and configure **shortcut** statement for SPRING routes using family inet (for IPv4 OSPF routes) or family inet-mpls (for IPv4 L-OSPF routes).

[See: [Understanding Adjacency Segments, Anycast Segments, and Configurable SRGB in SPRING](#).]

- **Support for configurable SRGB used by SPRING in OSPF protocols (MX Series)**— Starting in Junos OS Release 19.1R1, you can configure the segment routing global block (SRGB) range label used by segment routing. Labels from this range are used for segment routing functionality in OSPF domain.

The SRGB is a range of the label values used in the segment routing. Prior to Junos OS Release 19.1R1, you could not configure the range for the SRGB block.

Locally you can configure `srgb start-label <label-range> index-range <index-range>` command under `[edit protocols ospf source-packet-routing]` hierarchy or globally under `[edit protocols mpls label-range]` hierarchy.

Following are the SRGB precedences for OSPF protocol:

- SRGB under OSPF

- SRGB under MPLS
- Node-segment implementation of 256 label block

[See: [source-packet-routing \(Protocols IS-IS and OSPF\)](#).]

- **Support for static adjacency segment identifier in OSPF protocols (MX Series)**—Starting in Junos OS Release 19.1R1, static adjacency segment identifiers (SIDs) are supported for OSPFv2 protocols.

For static adjacency SIDs, the labels are picked from either a static reserved label pool or from an OSPF segment routing global block (SRGB). You can reserve a label range to be used for static allocation of labels using the following configuration: **set protocols mpls label-range static-label-range start-value end-value**

The static pool can be used by any protocol to allocate a label in this range. You need to ensure that no two protocols use the same static label. OSPF adjacency SIDs can be allocated from this label block through the configuration using the keyword **label**.

[See: [Static Adjacency Segment Identifier for OSPF](#).]

- **Support for export of BGP Adjacency-RIB-Out through BGP Monitoring Protocol (BMP) (MX Series)**—Starting in Junos OS Release 19.1R1, BMP is enhanced to support route monitoring of pre and post **rib-out** policy.

You can configure **post-policy** and **pre-policy** under **rib-out** statement at **[edit protocols bgp bmp]**, **[edit protocols bgp group group-name bmp]**, and **[edit protocols bgp group group-name neighbor address bmp]** hierarchies.

NOTE: The default monitoring mode of rib-out is **pre-policy**.

[See: [Understanding the BGP Monitoring Protocol](#).]

- **Support for TCP authentication to BGP peers (MX Series)**— Starting in Release 19.1R1, Junos OS extends support for TCP authentication to BGP peers that are discovered through allowed prefix subnets configured in a BGP group.

In releases before Junos OS Release 19.1, BGP supports TCP authentication at the **[edit protocols bgp group group-name neighbor address]** and **[edit protocols bgp group group-name]** hierarchy levels. Starting in Junos OS Release 19.1, you can configure TCP authentication under allow statements at the **[edit protocols bgp group group-name dynamic-neighbor dyn-name]** hierarchy level.

[See: [Understanding Router Authentication for BGP](#).]

- **Support for stitching of OSPF LDP and segment routing (MX Series)**—Starting in Junos OS Release 19.1R1, segment routing-LDP border router can stitch segment routing traffic to LDP next hop and vice versa.

In an LDP network with deployment of segment routing, there can be islands of devices that support either only LDP, or only segment routing. For the devices to interwork, the LDP mapping server feature is required to be configured on any device in the segment routing network.

[See: [LDP Mapping Server for Interoperability of Segment Routing with LDP Overview](#).]

- **Support for BGP link-state distribution with SPRING extensions (MX Series)**—Starting in Junos OS Release 19.1R1, BGP link-state extensions export segment routing topology information to software-defined networking controllers. Controllers can get the topology information by either being a part of an interior gateway protocol (IGP) domain or through BGP link-state distribution.

BGP link-state distribution is supported on inter-domain networks and provides a scalable mechanism to export the topology information. This feature benefits networks that are moving to source packet routing in networking (SPRING) but also have RSVP deployed, and continue to use both SPRING and RSVP in their networks.

In this release, OSPF link-state protocol is supported which pushes SPRING information to the BGP link-state address family.

[See [Link-State Distribution Using BGP Overview](#).]

- **MPLS transit route installation as primary MPLS fast reroute (FRR) for BGP labeled unicast prefixes (MX Series)**—Starting in Junos OS Release 19.1R1, when a peer autonomous system (AS) boundary router or a link fails, traffic traversing through an inter-AS link can be rerouted provided a loop-free path is available. In networks with node protection enabled, MPLS transit routes are installed as primary backup path for BGP labeled unicast prefixes learned from external BGP multi-hop sessions. This feature facilitates quicker route resolution and BGP convergence for BGP labeled unicast prefixes.

To enable node protection in an inter-AS environment for BGP labeled unicast prefixes, include the existing configuration statement **protection** at the `[edit protocols bgp group family inet labeled-unicast]` hierarchy level in **enhanced-ip network-services** mode.

- **Support for creating IS-IS topology-independent LFA for prefix-SIDs learned from LDP mapping server (MX Series)**—Starting in Junos OS Release 19.1R1, you can configure a point of local repair to create a topology-independent loop-free alternate backup path for prefix-SIDs derived from LDP mapping server advertisements in an IS-IS network. In a network configured with segment routing, IS-IS uses the LDP mapping server advertisements to derive prefix-SIDs. LDP Mapping server advertisements for IPv6 are currently not supported.

To attach flags to LDP mapping server advertisements, include the **attached** statement at the `[edit routing-options source-packet-routing mapping-server-entry mapping-server-name]` hierarchy level.

[See [prefix-segment-range](#).]

Services Applications

- **Support for tunnel interfaces on the MPC10E line card (MX Series)**—Starting in Junos OS Release 19.1R1, Junos OS supports three tunnel interfaces: generic routing encapsulation (GRE) tunnel, logical tunnel (LT), and virtual tunnel (VT) on the MPC10E line card.

- The GRE tunnel interface supports the **tunnel** statement with these options: **destination**, **key**, **source**, **traffic-class** and **ttl**. The **copy-tos-to-outer-ip-header** statement is also supported.
- The LT interface supports **family inet**, **family inet6**, and **family iso** options. The **encapsulation** statement supports the Ethernet and VLAN physical interface options only.
- The VT interface supports the **family inet** option only.

[See [Tunnel Services Overview](#)]

- **Support for Port Mirroring on the MPC10E line card (MX Series)**—Starting in Junos OS Release 19.1R1, Junos OS supports port mirroring on the MPC10E line card. The MPC10E supports IPv4 (inet) and IPv6 (inet6) address families only.

[See [Configuring Port Mirroring](#)]

- **Support for inline flow monitoring on the MPE10E line card (MX Series)**—Starting in Junos OS Release 19.1R1, Junos OS supports inline active flow monitoring. Inline active flow monitoring supports version 9 and IPFIX flow collection templates. Version 9 template is supported for IPv4, IPv6, MPLS, and MPLS-IPv4. IPFIX template is supported for IPv4, IPv6, MPLS, MPLS-IPv4, and VPLS flows. Both IPFIX and version 9 templates use UDP as the transport protocol.

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

- **Support for automatic restart of Two-Way Active Measurement Protocol (TWAMP) Client**—Starting in Junos OS Release 19.1R1, the TWAMP client restarts automatically after a network failure, a configuration change, or an IP connectivity issue. However, for the client to reconnect to the TWAMP server automatically, you must use 0 as the **test-count** value in the **set rpm twamp client control-connection test-count** command. Also, at the TWAMP server side, the default value of **max-connection-duration** in the **set rpm twamp server max-connection-duration** must also be 0. You can display the test results after the network recovers, or after the server is reachable, by using the **set services rpm twamp client control-connection c1 persistent-results** command.

[See [Understanding TWAMP Auto-Restart](#)].

- **Support for Layer 2 services over GRE tunnel interfaces with IPv6 transport (MX Series routers with MPCs)**—Starting in Release 19.1R1, Junos OS supports Layer 2 Ethernet services over GRE interfaces with IPv6 traffic. After GRE encapsulates the packets, it redirects them to an intermediate host, where they are de-encapsulated and routed to their final destination. Support for bridging over GRE enables you to configure bridge domain families on gr- interfaces and also enable integrated routing and bridging (IRB) on gr- interfaces. To configure the bridge domain family on gr- interfaces, include the **family bridge** statement at the **[edit interfaces gr-fpc/pic/port unit logical-unit-number]** hierarchy level.

[See [Layer 2 Services over GRE Tunnel Interfaces on MX Series with MPCs](#)].

Software Defined Networking (SDN)

- **Support for in-chassis Junos Node Slicing (MX480, MX960, MX2010, and MX2020)**—Starting in Junos OS Release 19.1R1, Junos Node Slicing supports an in-chassis model, which allows all Junos Node Slicing components, such as Juniper Device Manager (JDM), base system (BSYS), as well as guest network

functions (GNFs), to run within the Routing Engine of the MX Series router. To configure in-chassis Junos Node Slicing, ensure that the MX Series router has one of the following Routing Engines installed:

- RE-S-2X00x6-128 (used in MX480 and MX960 routers)
- RE-MX200X8-128G (used in MX2010 and MX2020 routers)

[See [Junos Node Slicing Overview](#) and [Configuring MX Series Router to Operate in In-Chassis Mode](#).]

- **Support for VXLAN on GNFs (MX480, MX960, MX2010, MX2020, and MX2008)**—Starting in Junos OS Release 19.1R1, guest network functions (GNFs) support EVPN with VXLAN encapsulation. This support enables you to configure GNFs to function as VXLAN Layer 2 or Layer 3 gateways. This support is also available on MX Series routers in LAN mode.

[See [Understanding EVPN with VXLAN Data Plane Encapsulation](#) and [Components of Junos Node Slicing](#).]

- **Abstracted fabric interface support for MS-MPC, 16X10GE MPC, MPC2E, MPC3E, MPC4E (MX480, MX960, MX2010, MX2020, and MX2008)**—Starting in Junos OS Release 19.1R1, Abstracted fabric (af) interfaces interoperate with the following line cards:
 - Multiservices MPC (MS-MPC)
 - 16x10GE MPC
 - MPC2E
 - MPC3E
 - 32x10GE MPC4E
 - 2x100GE + 8x10GE MPC4E

An abstracted fabric interface is a pseudointerface that facilitates routing control and management traffic between guest network functions (GNFs) through the switch fabric.

[See [Abstracted Fabric \(AF\) Interface](#).]

- **MS-MIC and MS-MPC support for in-chassis Junos Node Slicing (MX480, MX960, MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 19.1R1, in-chassis Junos Node Slicing supports assignment of MS-MICs and MS-MPCs to guest network functions (GNFs). MS-MICs and MS-MPCs provide improved scaling and high performance, and possess enhanced memory and processing capabilities. The MS-MIC supports the Layer 3 services such as stateful firewall, NAT, IPsec, active flow monitoring, RPM, and graceful Routing Engine switchover (GRES). In-chassis Junos Node Slicing also support inline Layer 2 and Layer 3 services.

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

- **Software resiliency support for in-chassis Junos Node Slicing (MX480, MX960, MX2010, and MX2020)**—Starting in Junos OS Release 19.1R1, software resiliency is enabled for guest network functions (GNFs) in the in-chassis Junos Node Slicing model. Resiliency enables the software to recover from certain types of failures. The in-chassis model allows all Junos Node Slicing components, such as Juniper

Device Manager (JDM), base system (BSYS), as well as guest network functions (GNFs), to run within the Routing Engine of the MX Series router.

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

- **Multiversion software support for in-chassis Junos Node Slicing (MX480, MX960, MX2010, and MX2020)**—Starting in Junos OS Release 19.1R1, in-chassis Junos Node Slicing supports multi-version software interoperability, enabling the BSYS to interoperate with a guest network function (GNF), which runs a Junos OS version that is later than the software version on the base system (BSYS). This feature supports a difference of up to two versions between the GNF and the BSYS. That is, the GNF software can be up to two versions later than the BSYS software.

NOTE: The multiversion software compatibility support is limited to major releases only.

[See [Understanding Multi-Version Software Compatibility](#).]

- **Programmable flexible VXLAN tunnels (MX80, MX104, MX204, MX10003, and vMX)**—Starting in Junos OS Release 19.1R1, we support flexible VXLAN tunnels in a data center environment that includes one or more controllers. In this environment, one or more of the supported MX Series routers can function as data center edge gateways that exchange Layer 2 traffic with hosts in a data center. Through the use of static routes and tunnel encapsulation and de-encapsulation profiles, the Layer 2 traffic is dynamically tunneled over an intervening IPv4 or IPv6 network.

The controllers in the data center environment enable you to program a large volume of static routes and tunnel profiles on the gateway devices through the Juniper Extension Toolkit (JET) APIs.

[See [Understanding Programmable Flexible VXLAN Tunnels](#) and the [JET API Guide](#)]

Subscriber Management and Services

- **Control plane resiliency enhancements (MX Series)**—Starting in Junos OS Release 19.1R1, the following enhancements are available:
 - The master and standby Routing Engines exchange detailed information about session database replication. This exchange enables the Routing Engines to better determine whether the replication is correct.
 - You can configure the router to detect shared memory corruption and to automatically recover by rebooting the master or standby Routing Engine, or both. In earlier releases, a manual reboot is required to clear the corrupted shared memory; otherwise, it remains corrupted, causing processes that share the memory to generate core errors.
 - You can monitor Routing Engine resiliency with the new **show system subscriber-management resiliency** command. The **summary** version indicates whether the system is functioning normally or an unexpected condition exists. The **detail** and **extensive** versions provide detailed information about the shared memory per Routing Engine.

[See [Junos OS Enhanced Subscriber Management](#) and [show system subscriber-management resiliency](#).]

- **Subscriber management support for in-chassis Junos Node Slicing (MX480, MX960, MX2010, and MX2020)**—Starting in Junos OS Release 19.1R1, in-chassis Junos Node Slicing supports 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.

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

- **DHCP active leasequery for live updates of binding information (MX Series)**—Starting in Junos OS Release 19.1R1, you can configure active leasequery so that DHCP servers can provide an update to DHCP relay agents whenever the DHCP binding information changes. Individual and bulk leasequery provide updates only in a response to a query; subsequent changes are not reported to the relay agent until another query is made. Active leasequery also enables redundancy between relay agents to restore subscriber information if one of the peer relay agents reboots.

[See [DHCP Leasequery Methods](#).]

- **Display RPF check statistics for dynamic logical interfaces (MX Series)**—Starting in Junos OS Release 19.1R1, the **show interfaces statistics *logical-interface-name* detail** command can display byte and packet statistics for unicast RPF failures. These statistics are only displayed for dynamic IPv4 or IPv6 logical interfaces where RPF check is configured with the **rpf-check** or **rpf-check mode loose** statement. The **clear interfaces statistics *logical-interface-name*** command clears RPF statistics.

[See [Unicast RPF in Dynamic Profiles for Subscriber Interfaces](#).]

- **Additional encapsulations added to pseudowire subscriber logical interfaces (MX Series with MPC and MIC)**—Currently, the only supported encapsulation type on the pseudowire subscriber interfaces include:

- **Transport logical interfaces**—Circuit cross-connect (CCC) encapsulation.
- **Service logical interfaces:**
 - Ethernet VPLS encapsulation
 - VLAN bridge encapsulation
 - VLAN VPLS encapsulation

Starting in Junos OS Release 19.1R1, in addition to the existing encapsulation types, the following support is provided:

- **Transport logical interfaces**—Ethernet VPLS encapsulation, and provision for terminating the interface on the l2backhaul-vpn routing-instance.
- **Service logical interfaces**—Circuit cross-connect (CCC) encapsulation, and provision for terminating the interface on locally switched Layer 2 circuits.

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

- **Insert identifier tags in HTTP GET headers (MX Series)**—Starting in Junos OS Release 19.1R1, you can configure HTTP redirect service filters to insert tags into the headers of HTTP GET messages. You can specify one or more destination addresses in the service rule to identify traffic for tagging. The tagged message is forwarded to the HTTP server where the server can accept or reject access based on the tag values.

[See [Inserting GET Header Tags That the HTTP Server Can Use to Control Content Access](#).]

System Logging

- **Support for TCP/TLS transport for syslog (MX240, MX480, and MX960)**—Starting with Junos OS Release 19.1R1, you can configure multiple TLS syslog servers for a service on the MS-MPC or MS-MIC services cards. You can configure a maximum of four syslog servers for each set of services, and send encrypted data to the servers. The source address for the logs sent to remote hosts uses the configured source address of TCP/TLS host. See [TCP/TLS Transport Protocol for Syslog Messages Configuration Overview](#).

SEE ALSO

Changes in Behavior and Syntax	90
Known Behavior	96
Known Issues	99
Resolved Issues	110
Documentation Updates	123
Migration, Upgrade, and Downgrade Instructions	123
Product Compatibility	130

Changes in Behavior and Syntax

IN THIS SECTION

- [EVPN](#) | [91](#)
- [General Routing](#) | [91](#)
- [Interfaces and Chassis](#) | [91](#)
- [MPLS](#) | [93](#)
- [Network Management and Monitoring](#) | [94](#)
- [Network Operations and Troubleshooting Automation](#) | [94](#)

- Routing Protocols | 94
- Services Applications | 94
- Software-Defined Networking (SDN) | 95
- Subscriber Management and Services | 95
- User Interface and Configuration | 95

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 19.1R1 for MX Series routers.

EVPN

- **Changes in encoding the ESI label field (MX Series)**—Starting in 19.1R1, Junos OS switched from using lower-order bits to higher-order bits in encoding the ESI label field. This results in BUM traffic loss and duplication in traffic. If you encounter this, and you wish to use a mix of Junos OS releases, you must include the **es-label-oldstyle** statement at the **[edit routing-instances *routing-instance-name* protocols evpn]** hierarchy on the device that is running the Junos OS release that supports higher-order bit encoding of the ESI label.

General Routing

- **Root XML tag change for show rsvp pop-and-forward | display xml command (MX480)**—We’ve changed the root XML tag for the show rsvp pop-and-forward | display xml command to rsvp-pop-and-fwd-information to make it consistent with the XML tag convention. In earlier releases, the command output displays rsvp-pop-and-fwd-info XML tag. Update the scripts with the rsvp-pop-and-fwd-info XML tag to reflect the new rsvp-pop-and-fwd-information XML tag.

[See [Junos XML API Explorer - Operational Tags.](#)]

Interfaces and Chassis

- In MX204 routers, the error messages are logged when **vlan-tagging** for a trunk interface that is not configured. These error messages were previously logged with severity level “critical” even though they were not critical enough to require immediate action. The maximum transmission unit (MTU) of interface with or without VLAN-tagging is now logged in as the informational error message (instead of critical error message).
- **IRB not supported on pseudowire subscriber (PS) logical Interface in bridge-domain (MX Series)**—In Junos OS Release 19.1R1, integrated routing and bridging (IRB) is not supported on pseudowire subscriber

(PS) logical Interface. Hence, you cannot add IRB to a bridge domain with PS interface, that is, you cannot configure IRB and PS interface in the same bridge domain.

Note that adding IRB to a bridge domain having pseudowire subscriber (PS) logical interface causes kernel crash and continuous reboot of the router until the configuration is rolled back.

NOTE: IRB is not supported on PS only in bridge-domain.

[See [bridge-domain](#).]

- **Support for MAP-E encapsulation and de-encapsulation on inline service interfaces (MX2010)**—Starting in Junos OS Release 19.1R1, the MX2010 routers support encapsulation and de-encapsulation of the following ICMP message types for inline service (si) interfaces:
 - Time exceeded (type 11)
 - Destination unreachable (type 3)
 - Source quench (type 4)
 - Parameter problem (type 12)
 - Address mask request and Address mask reply (type 17 and type 18)
 - Redirect (type 5)
- **New XML tag element <lacp-hold-up-state> added in show lacp interfaces XML display (MX Series)**—Starting in Junos OS Release 19.1R1, the **show lacp interfaces | display xml** command displays a new XML tag element <lacp-hold-up-state>. The <lacp-hold-up-state> displays the time interval an interface holds before it changes from state, down to up. In earlier Junos OS releases, the LACP hold up the information for all interfaces was in a single <lacp-hold-up-information> XML tag. Now, for each interface it is displayed in a separate <lacp-hold-up-information> XML tag.
- **Support for creating Layer 2 logical interfaces independently (MX Series)**—In Junos OS Releases 18.4R1, 18.4R2, 19.1R1, 19.1R2, and later, MX Series routers support creating Layer 2 logical interface independent of Layer 2 routing instance type. That is, you can configure and commit the Layer 2 logical interfaces separately and add the interface to the bridge domain or Ethernet VPN (EVPN) routing instance separately. Note that the Layer 2 logical interfaces works fine only when the interface is added to the bridge domain or EVPN routing instance.

In the earlier Junos OS releases, when a Layer 2 logical interface configuration (units with encapsulation vlan-bridge configuration) is used, then the logical interface must be added as part of a bridge-domain or EVPN routing instance for the commit to succeed.
- **Support to get Optics loopback status for QSFP-100GE-DWDM2 transceivers (MX Series)**—Starting in Junos OS Releases 19.1R1, on MX Series routers, you can get the optics loopback status of QSFP-100GE-DWDM2 transceivers along with the regular Ethernet loopback status by issuing the **show interfaces interface-name** or **show interfaces interface-name brief** command. The new output field **Optics**

Loopback is added under **Link-level type** when the **show interfaces *interface-name*** CLI command is executed.

MPLS

- Starting in Junos OS Release 18.4R1 and 19.1R1, the remote procedure call (RPC) protocol XML tag for **mpls-label-value** is renamed as **mpls-history-label-value**, **mpls-usage-label-value**, and **mpls-label-id-value** depending on the context of command usage.
- **New debug statistics counter (MX Series)**—The **show system statistics mpls** command has a new output field, called **Packets dropped, over p2mp composite nexthop**, to record the packet drops over composite point-to-multipoint next hops.

Network Management and Monitoring

- **NETCONF <kill-session> operation returns different values in <rpc-error> when the session identifier is equal to the current session ID (MX Series)**—Starting in Junos OS Release 19.1R1, when you execute the <kill-session> NETCONF operation and the session identifier is equal to the current session ID, the values of the <error-type> and <error-tag> elements in the resulting <rpc-error> are **application** and **invalid-value**, respectively. In earlier releases, the <error-type> and <error-tag> values are **protocol** and **operation-failed**.

[See [<kill-session>](#).]

Network Operations and Troubleshooting Automation

- Starting in Junos OS Release 19.1, the RPC XML tag for **mpls-label-value** is renamed as **mpls-history-label-value**, **mpls-usage-label-value**, and **mpls-label-id-value** depending on the context of command usage.

Routing Protocols

- **Support for BGP LU link protection for a multihop EBGp peer (MX-Series)**—Starting in Junos OS Release 19.1R1, you can enable BGP Labeled unicast protection for an indirect next hop for logical-interface-based FRR. In earlier Junos Releases, Junos OS did not compute a backup path for the active indirect next hop failure and caused link failure for EBGp multihop cases where EBGp is chosen as a primary route for BGP LU protection on affected routes.

To configure BGP link protection for a multihop EBGp peer, enable **protection** at the **[edit protocols bgp group group-name family inet labeled-unicast]** hierarchy level.

Services Applications

- **Change in error message displayed while fragmenting or defragmenting IPv6 GRE tunnel interface (MX Series routers)**—In Junos OS Release 19.1R1, on an IPv6 GRE tunnel interface, when you enable fragmentation using the **allow-fragmentation** command or disable fragmentation using the **do-not-fragment** command, the following error message is displayed:

Fragmentation for V6 tunnels is not supported

In earlier Junos OS releases, the following message was displayed:

dcd_config_ifl_tunnel:Fragmentation for V6 tunnels is notsupported

- **Support for host generated traffic on a GRE over GRE tunnel (MX Series)**—In Junos OS Release 19.1R1, you can send host generated traffic on a GRE over GRE tunnel. However, when path maximum transmission unit (PMTU) is updated for the outer GRE tunnel, MTU for inner GRE tunnel is not corrected.

Software-Defined Networking (SDN)

- Starting in Junos OS Release 18.2X75-D30 and 19.1R1, the maximum value for service identifier (SID) depth for PCEP segment routing (SR) LSP has been increased to more than 5 labels. The supported range of **max-sid-depth** is 1 through 16 with a default value of 5 labels.

[See [pce](#).]

Subscriber Management and Services

- **ICMP error message rate limit increased (MX Series)**—Starting in Junos OS Release 19.1R1, the maximum rate limit for generating ICMP messages for IPv4 and IPv6 packet errors is increased from 50 pps to 1000 pps. The rate limit applies only to non-ttl-expired packets.

[See [Configuring the Rate Limit for ICMPv4 Error Messages](#) and [Configuring the Rate Limit for ICMPv6 Error Messages](#),]

- **Subscribers allowed to log in with bad framed route (MX Series)**—Starting in Junos OS Release 19.1R1, users are allowed to log in if the framed route received from RADIUS is bad; for example, if the format is incorrect. In earlier releases, the subscriber is not allowed to log in. For customers that use multiple framed routes, the new behavior enables the subscriber to have partial access to the network using the routes that are accepted instead of not being allowed any access.
- **Changing attributes of physical interface with active subscribers (MX Series)**—Starting in Junos OS Release 19.1R2, the commit check fails when you change any attribute of the physical interface, such as the MTU, when subscribers are active. This affects only aggregated Ethernet physical interfaces with targeted distribution configured. In earlier releases, the commit check does not fail and the attribute change brings down the physical interface and all subscribers using that interface.

User Interface and Configuration

- **Options for monitor traffic interfaces statement added (MX Series)**—Starting in Junos OS Release 19.1R1, the options **write-file** and **read-file** under the **monitor traffic** command are included in the visible CLI.

[See [monitor traffic](#).]

SEE ALSO

New and Changed Features 69
Known Behavior 96
Known Issues 99

[Resolved Issues | 110](#)

[Documentation Updates | 123](#)

[Migration, Upgrade, and Downgrade Instructions | 123](#)

[Product Compatibility | 130](#)

Known Behavior

IN THIS SECTION

- [Forwarding and Sampling | 96](#)
- [General Routing | 96](#)
- [Infrastructure | 97](#)
- [MPLS | 97](#)
- [Platform and Infrastructure | 97](#)
- [Routing Protocols | 97](#)
- [Software Defined Networking | 97](#)
- [Subscriber Management and Services | 98](#)

This section contains the known behavior, system maximums, and limitations in hardware and software in Junos OS Release 19.1R1 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

- LTS subscriber statistics are reported to RADIUS. [PR1383354](#)

General Routing

- CFM is not supported for Layer 2-over-GRE tunnel. CCM can pass through as transit traffic through GRE interfaces transparently using datapath. Link trace functionality uses mac-learning and re-injecting LTM on GRE interface in case the bridge is configured with CFM. This is not a supported feature. [PR1275833](#)

- When SRTE policies have segment lists that have a single label or three or more labels, the IS-IS interface statistics are not incremented even when SRTE routes take these IS-IS next-hops. The kstat based states are enabled in IS-IS by following command: **set protocols isis source-packet-routing traffic-statistics**. [PR1410682](#)

Infrastructure

- On MX480 routers, after upgrade to Junos OS Release 15.1 and later, the failure message about **smartd[xxxx]: Device: /dev/ada1, failed to read SMART Attribute Data** might appear in the log. [PR1333855](#)

MPLS

- With NSR enabled, when the master rpd is restarted, occasionally, out-of-order add and delete messages can arrive on the backup Routing Engine, causing label assignment collisions leading the backup rpd to crash. [PR1401813](#)

Platform and Infrastructure

- On MX480 routers configured as type-5 route peers, when only peer 1 advertises routes, that peer might not install the de-encapsulated next-hop route. As a result, type-5 encapsulated traffic that is sent by peer 2 is dropped until peer 2 advertises any type-5 route. As a workaround, configure a static route pointing to discard on peer 2 and advertise that route as a type-5 route to peer 1. [PR1386423](#)

Routing Protocols

- When 32,000 SRTE policies are configured at once, during configuration there might be scheduler slips. [PR1339829](#)

Software Defined Networking

- The MX Series platform type of the guest network function (GNF) configured on an MX chassis will not automatically change if the Routing Engine is installed on a different MX chassis type. To fix this issue, you need to delete the GNF and configure it from the start on the new Chassis in which Routing Engine is installed.
- When guest network functions (GNFs) are rebooted for different reasons, the **show chassis routing-engine** may incorrectly display the reboot reason as **Router rebooted after a normal shutdown**. To find the actual reboot reasons, refer to the log messages of GNFs.

- External Ethernet port LEDs on Control Board of MX2020 and MX2010 routers do not turn off when network-slices configuration is deleted or deactivated.
- If you try to install Juniper Device Manager (JDM) after performing **request vmhost zeroize**, the installation will be unsuccessful. As a workaround, you can delete the JDM and install it again.
- The PS interface maximum transmission unit (MTU) size at times will have incorrect default value. As a workaround, you can delete the PS interface and configure it again.
- Junos OS Release 19.1R1 does not interoperate with earlier releases of Junos OS that support Junos node slicing. To run the 19.1R1 version of Junos node slicing on any GNF, the BSYS and all other GNFs must also run Junos OS 19.1R1.

Subscriber Management and Services

- For dual-stacked clients over the same PPP over L2TP LNS session, enhanced subscriber management does not support configurations where both of the following are true:
 - The CPE sends separate DHCPv6 solicit messages for the IA_NA and the IA_PD.
 - The solicit messages specify a type 2 or type 3 DUID (link-layer address).

As a workaround, you must configure the CPE to send a single solicit message for both IA_NA and IA_PD when the other configuration elements are present.

SEE ALSO

[New and Changed Features | 69](#)

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

[Known Issues | 99](#)

[Resolved Issues | 110](#)

[Documentation Updates | 123](#)

[Migration, Upgrade, and Downgrade Instructions | 123](#)

[Product Compatibility | 130](#)

Known Issues

IN THIS SECTION

- [EVPN | 99](#)
- [Forwarding and Sampling | 99](#)
- [General Routing | 100](#)
- [Infrastructure | 105](#)
- [Interfaces and Chassis | 105](#)
- [Layer 2 Ethernet Services | 106](#)
- [MPLS | 106](#)
- [Network Management and Monitoring | 107](#)
- [Platform and Infrastructure | 107](#)
- [Routing Policy and Firewall Filters | 107](#)
- [Routing Protocols | 107](#)
- [Subscriber Access Management | 109](#)
- [User Interface and Configuration | 109](#)
- [VPNs | 109](#)

This section lists the known issues in hardware and software in Junos OS Release 19.1R1 for MX Series routers.

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

EVPN

- An error is observed when you execute the **vlan ping overlay** rpc command. It works through CLI but not through rpc . [PR1373025](#)
- If the parameter **auto** is set to the **vrf-target** statemnt within an instance-type of EVPN/virtual-switch, the rpd process would crash after deactivating the autonomous system (AS) configured. [PR1381940](#)

Forwarding and Sampling

- If the value of **mac-table-size** of a given VLAN that is carrying traffic is changed to default, then the layer 2 forward table (IFL-List) needs to be re-associated with flush-list that keeps the newest MAC

list pushed by the Route Engine, then the IFL-List must be deleted for this re-association. However, when the MAC entries are deleted, their flags might still remain in the IFL-List, that causes the MAC deletion failure, also the update of the flush-list might get stuck. Consequently, all FPC might reboot.

[PR1386768](#)

- For Junos OS Release 18.4R1, if IPv4 prefix is added on a prefix list referred by an IPv6 firewall filter, then the log message **Prefix-List [Block-Host] in Filter [Protect_V6] not having any relevant prefixes , Match [from prefix-list Block-Host] might be optimized** will not be seen in this particular release.

[PR1395923](#)

- For Junos OS Release 19.1R1, in case of physical interface policer for ip-option traffic, the traffic rate is found to be more than 10 percent. [PR1398728](#)

General Routing

- When performing a Routing Engine switchover, without the support of nonstop routing (NSR) , the l2cpd daemon might occasionally report a slip in its scheduled run of a few seconds (1 to 10) and print a log message as follows: **Aug 1 10:41:21 mx9601 l2cpd[32770]: JTASK_SCHED_SLIP: 8 sec scheduler slip, user: 0 sec 2180 usec, system: 0 sec, 2188 usec This delayed run has no functionality nor operational effect to any of the L2 protocols controlled by L2CPD because STP task delegates transmit/receive bpdus to a separate dedicated PPMD daemon, and LLDP task's transmit/receive PDUs are dealt from daemon itself but the advertisement-interval is 30 seconds, with hold-timer for neighbors LLDPDU being 120 seconds, so the time to recover the few seconds of slips is plenty and enough to absorb it.**

[PR1203977](#)

- Performance of X710 NIC is lower compared to that of 82599 NIC. The 40-Gigabit Ethernet line rate can be achieved at 512-byte packet size for X710 NIC as compared to 256 bytes for 82599 NIC. [PR1281366](#)
- If a vmhost snapshot is taken on an alternate disk and there is no further vmhost software image upgrade, the expectation is that if the current vmhost image gets corrupted, the system will reboot with the alternate disk so that you can recover the primary disk to restore the state. However, when the corruption is with the host root file system, the node is booting with the previous vmhost software instead of booting from the alternate disk. [PR1281554](#)
- The Routing Engine gets stuck and reboots from the other SSD after vmhost reboot. You must boot the Routing Engine from the primary SSD. [PR1295219](#)
- The **show dynamic-tunnels database summary** command does not show an accurate tunnels summary during the time the anchor Packet Forwarding Engine line card is not in up state. As a workaround, use the **show dynamic-tunnels database** and **show dynamic-tunnels database terse** commands. [PR1314763](#)
- MPLSoGRE dynamic tunnel localization does not work when **chained composite nexthop** is enabled. This command does not bring in a lot of gain because TCNH is based on the ingress rewrite premise. Without this command things work fine. [PR1318984](#)

- In JDM, (running on the secondary server) the jdmd daemon might generate core files if GNF add-image is aborted by pressing Ctrl+c. [PR1321803](#)
- With regard to FPC restart or Virtual Chassis splits, the design of MX Series Virtual Chassis infrastructure relies on the integrity of the TCP connections, and the reactions to a failure situation might be handled gracefully. For example, the TCP connection times out because of jlock hog crossing boundary value (5 seconds), causing bad consequences in the MX Series Virtual Chassis. As a workaround, enable the marker infrastructure on the MX Series Virtual Chassis setup. [PR1332765](#)
- The output of the **show class-of-service fabric statistics** command now includes traffic that was dropped because of internal errors in the drop counts. [PR1338647](#)
- The first packet pertaining to the J-Flow Packet Forwarding Engine sensor in UDP mode is missing after the line card reboots on the MX150 router. [PR1344755](#)
- With GRES enabled in a subscriber environment, if subscribers are logging in or logging out quickly, the service sessions in the session database of the backup Routing Engine might be leaked. If the problem is not detected for long enough, the backup Routing Engine might not be able to come back into synchronization with the master Routing Engine and will not be ready for GRES. [PR1346300](#)
- During unified ISSU that warrants host upgrade, if the router is configured with 8 million IPv4 or IPv6 routes or more, the unified ISSU operation might fail, resulting in FPC restart. [PR1348825](#)
- In some cases, online insertion and removal (OIR) of a MIC on an FPC can lead the traffic destined to the FPC to be discarded without notification. The only way to recover from this is to restart the FPC. The issue will not be seen if you use the corresponding CLI commands to turn the MIC offline and then online. [PR1350103](#)
- The issue only occurs on aggregated Ethernet link deactivate/activate, which means that the LAG interface is deleted from the system and created again. But then, issue does not happen on de-activating/activating the link manually or by running this individual case in the script. There is no traffic loss. The traffic will continue to use the kackup link. The aggregated Ethernet link up/down case is working as expected. Forwarding allocates a hardware selector for every group for local-repair which will be shared by multiple unilist next-hops (A next-hop with active and backup gateways using the primary and backup logical interfaces). The selector is getting stuck in rerouted state. There is no traffic loss but the traffic is flowing through the backup link even after the primary aggregated Ethernet link is created again. The problem seems be with unilist->indirect->hold to unilist->indirect->unicast state transition during the deactivate/activate. As a workaround, enable the **vty** command to change the unilist hold behavior. [PR1354786](#)
- The configurations of bridging routing instances having aggregated Ethernet logical interfaces (6400 IFLs) and IRB instances, all from a single FPC, the CPU utilization of the FPC stays at 100 percent for 4 minutes. The behavior from PFEMAN of the FPC has the processing time spiked on IF IPCs and this seems to be the case of MPC7E starting in Junos OS Release 16.1R1 (or even earlier). After 4 minutes, the CPU utilization comes down and the FPC is normal. Therefore, this scale configuration on MPC7E takes settling time of 4+ minutes. [PR1359286](#)

- When rpd reads next hops from the kernel on restart, for INH -> FWD NH{List NH} -> {Chain NH} scenario, the rpd should not create an old-style list next hop for the forwarding next hop. [PR1360354](#)
- In Junos OS releases that support ephemeral configuration databases, the configuration commit time might be delayed by ~30 seconds as the rpd validates the new configuration. If the synchronized commit is used, then there is a time delay of ~1 min. [PR1364621](#)
- It is possible for a GNF with rosen6 multicast to display stuck KRT queue entries after recovery from a dual Routing Engine reboot at the BSYS. [PR1367849](#)
- When FPC is booting up (either during unified ISSU or router reboot or FPC restart), i2c timeout errors for SFP can be noticed. These errors are seen as i2c action is not completed because the device was busy. Once the card is up, all the i2c transactions to the device work correctly, so no periodic failure is observed. There is no functional impact and these errors can be ignored. [PR1369382](#)
- The voltage high alarm might not be cleared when voltage level comes back to normal for MIC on MPC5E. [PR1370337](#)
- If an interface is configured with 128 prefix length for IPv6 address, the route learned over that interface might be marked as "dead" next-hop after the prefix length is changed from 128 to any other prefix length. [PR1380600](#)
- The interface filter statistics are not showing the input packet count/rejects and **show pfe statistics traffic** does not report for any normal discard. [PR1383579](#)
- Users can still issue the **set vmhost...** although **"permissions system-control** command that is not configured on the system class. [PR1383706](#)
- On MX Series routers enabled with subscriber scenario, if a large scale of subscribers (for example, more than 1000 subscribers) set up connections simultaneously, the setup rate might be 30 percent lower than expected. [PR1384722](#)
- In low-end 32-bit systems, rpd has a lower level of available memory. It is desired to have a log message to alert users when the average memory usage or transient memory usage exceeds thresholds. [PR1387465](#)
- During Zero Touch Provisioning (ZTP) process, the default route is being cleaned up by code. Because of this, if a static default route is configured in the initial configuration (configuration file downloaded from the file server for ZTP), the route will fail to work. This might lead to ZTP failure or a device access issue after ZTP. [PR1387724](#)
- The bbe-smgd process generates core files when the MTU configuration is changed while the subscribers are still logged in on the physical interface. The MTU configuration change should only be done when there are no subscribers logged in on the physical interface. Catastrophic configuration changes should be done only in maintenance mode, when no subscribers are on the physical interface. [PR1389611](#)
- In a Junos Fusion Provider Edge (MX Series) scenario, all the FPCs might restart after committing the changes to the VLAN/encapsulation on the extended port if the parameter **per-interface-per-member-link ingress** is configured for sourced routing statistic by using the **set protocols isis source-packet-routing sensor-based-stats per-interface-per-member-link ingress** command. [PR1392071](#)

- On MX2008 routers with MPC9E, in a line rate traffic with a redundant SFB2 scenario, if you offline one redundant SFB2, there might be tail or sometimes WRED drops in MPC9E, resulting in partial traffic loss. Under normal circumstances, the SFBs should be auto-failover if one of them fails, and there should be only a few packets dropped momentarily. [PR1395591](#)
- MPC card/afeb/tfeb with channelized OC MIC might crash and generate core files. [PR1396538](#)
- The rpd has facilities to attempt to trap certain classes of nonfatal bugs by continuing to run, but leaving a "soft" core file. Leaving a soft core is intended to be nondisruptive to routing and forwarding. [PR1396935](#)
- When the MoFRR feature is used in a scaled environment (in terms of number of routes and next hops), the actual convergence of multicast traffic might reach hundreds of milliseconds because of suboptimal handling of MoFRR forwarding states on the Packet Forwarding Engine level. [PR1399457](#)
- The **ether-pseudowire zero-control-word** configuration option under the **forwarding-options enhanced-hash-key family mpls** statement does not take affect in a Junos OS node Slicing setup. Although configured as: **set forwarding-options enhanced-hash-key family mpls ether-pseudowire zero-control-word**, the parameter is not passed to MPC9E line card. This can impact load balancing over abstract fabric (AF) interface when using Pseudowire Headend Termination (PWHT) in a Guest Network Function (GNF). [PR1400881](#)
- In a BGP-PIC instance, If a route (R1), resolves on top of a multipath route (R2), where R2 has primary and backup indirect next hops, results will be better if the backup leg is not used for resolution of R1. There is no impact on any existing CLI commands. The backup path is never used when primary path is available. [PR1401322](#)
- The **sample-frequency** data-type is changed from milliseconds to seconds. [PR1402197](#)
- After upgrading to Junos OS Release 17.2 or later, the **chained-composite-next-hop ingress l3vpn extended-space** statement cannot be configured anymore on a logical system. [PR1402390](#)
- MPC might generate core files after restarting an FPC that belongs to targeting aggregated Ethernet and host subscribers. [PR1405876](#)
- The rpd might crash after a nonforwarding route (that is, a route to an indirect next-hop association is not forwarding the indirect next hop) that is received from multiple protocols is resolved again by using the non-forwarding path. [PR1407408](#)
- The MIC-MACSEC-20GE supports Extended Packet Numbering (XPN) mode on 1-Gigabit Ethernet or 10-Gigabit Ethernet interfaces. [PR1409457](#)
- When a **clear pim join instance <inet name>all** command is issued on vMX based platforms including MX150, it might cause a riot crash. [PR1409527](#)
- For AFT-based line cards, FW upgrade for Inphi Cortina modules should use the updated versions of scripts that support these line cards. Old scripts will fail to perform FW upgrade. [PR1410133](#)
- 1). Only in the case that all the below conditions are met, the telemetry statistics will not account correctly for the traffic on SRTE-policies (both byte count and packet count), on PTX platforms, only: a. SRTE policy is uncolored (color attribute is not enabled for the SRTE policy) b. protocols isis

source-packet-routing sensor-based-stats per-interface-per-member-link configuration is enabled. c. The outgoing interface for the SRTE route is an aggregated interface. [PR1413680](#)

- When you perform unified ISSU with PPPoE subscribers on PS interface. After unified ISSU, traffic is getting affected as a result keepalive messages are also dropped and PPPoE session gets terminated. [PR1414608](#)
- It has been noted that a small number of tunneled subscribers may be terminated during unified ISSU to Junos OS Release 19.1R1 software due to momentary loss of IP connectivity between the LAC and LNS devices. [PR1414928](#)
- When the Routing Engine software is not able to access the fabric chip, then the corresponding plane goes into fault state. The following log message is observed in this issue case. **Mar 12 08:16:12 CHASSISD_FASIC_PIO_READ_ERROR: Fchip (CB 1, ID 1): read error in sfchip_init() for link#100 at address 0 in register FCHIP_FTOP_CONFIG** [PR1416814](#)
- With RPM enabled, RPM probe generated logs will not be logged under syslog. RPM functionality will not have any impact. [PR1421934](#)
- On MX1RU, when changing the PIC port profile configuration to default PIC mode from a configuration which has single PIC enabled, mqss errors are observed. In MX1RU, when there is a PIC mode, the PIC bounce handling in the Routing Engine verifies if high performance mode can be supported or not. Subsequently, the Routing Engine sends an IPC messages to FPC to configure the correct PIC mode. There is a possibility to see MQSS error during the PIC initialization. The user is expected to restart the FPC to recover from the MQSS error state. [PR1423215](#)
- Unifeid ISSU fails with **ERROR: insufficient space for /var/tmp/junos-install-mx-x86-64-19.2I-20190225_dev_common.0.1257.tgz** error. [PR1423404](#)
- MPC10: crash seen @ Ktree alloc (jnh_dfw_instance_add (filter_index=< optimized out>) at ../../../../src/pfe/common/applications/dfw/dfw_iff.c:1030 with inline + scale prefix filter. [PR1423709](#)
- Downstream on FHR is not changing from PE interface to XE interface due to improper encapsulation on the PE interface [jnh error invalid loopback pkt format]. [PR1423887](#)
- MPC10E: When the primary path of the mpls lsp is changed (from p1 to p2), traffic on the l2circuits running over these lsp are dropped at the NNI [PR1425358](#)
- Fast-Lookup-Filter does not work for the MPC10E line card. During installation, the **fast-lookup-filter** is converted internally to the Dmem filter. [PR1431451](#)

Infrastructure

- Image size for junos-install-media-usb-mx-x86-64 images have been increased by 400 MB. For USB upgrade, image is stored on and installed from that USB drive. Because the image size has increased, the installation fails due to lack of swap space on the device. Increasing the USB size would give required room for installation. [PR1423139](#)

Interfaces and Chassis

- Upgrading Junos OS Release 14.2R5 and later maintenance releases and Junos OS Release 16.1 and later mainline releases with CFM configuration might cause the cfm process to crash after upgrade. This is because of the presence of an old version of the `/var/db/cfm.db` file. [PR1281073](#)
- Lfm sessions toward scaled peers might flap during unified ISSU switchover phase. [PR1377761](#)
- As part of the Ethernet OAM programming the LM counters are allocated. When an interface is deleted, the Ethernet OAM LM counters need to be cleared. This is done as part of Ethernet OAM punt deletion. However, there are scenarios in which the punt deletion is received, but the logical interface is deleted in ukern. In this case, the Ethernet OAM next-hops are cleared but the LM counters are not freed. This can cause memory leak in jnh. This issue is seen for scaled configurations, repeated additions, and deletions of interface configurations when Ethernet OAM configuration is present [PR1396540](#)
- There might be memory leak on transportd when bulk SNMP polling is on done large-scale logical interfaces and a large number of traps is created due to interface flapping. The memory leak could cause the transportd to consume high CPU for a prolonged period. [PR1398967](#)
- Static demux0 logical interfaces do not come up after configuration change if the underlying interface is et- (100-Gigabit Ethernet). After a configuration change, et- interface gets flushed in order to reparse the configuration. During this, the device control daemon the (dcd) fails to create the dependency between the demux0 logical interfaces and the underlying et- interface, which results in flushing of the demux0 logical interfaces. This issue is seen only if the underlying interface is et-. For all other interfaces, this issue has been already addressed. This is day-1 issue. As a workaround, either restart dcd (or reboot the Routing Engine) to clear the problem or else use **commit full** instead of **commit** while committing new configurations. [PR1401026](#)
- On MX Series platforms, EX-SFP-1FE-LX SFP does not initialize with MIC-3D-20GE-SFP-E(EH). [PR1405271](#)
- When an unnumbered interface is binding to an interface which has more than one IP address and one of the IPs is deleted, the family inet of the unnumbered interface might be getting deleted. The issue results in traffic loss for all the services that rely on the family inet of the unnumbered interface. Configure preferred-source-address on the unnumbered interface will prevent deletion of the IP hence avoiding the deletion of the family inet of the unnumbered interface. [PR1412534](#)

Layer 2 Ethernet Services

- On MX Series routers, if a static demux interface over an underlying interface is configured, after the subscriber logs out, the accounting statistics are not cleared. [PR1383265](#)
- A jdhcpc subscriber loss is seen after performing unified ISSU to Junos OS Release 19.1R1. The issue is seen because as part of the unified ISSU, chassisd is killing ksyncd process in RE1 and as part of the cleanup, ksyncd is deleting the non default routing instances. jdhcpc is processing those events and deleting the clients on those routing instances. [PR1420982](#)

MPLS

- If the primary link goes down immediately after bypass (say FPC containing both primary & bypass or, both primary & bypass FPCs go down simultaneously) such that primary link goes down even before the PLR sends out any Path message after bypass down, then the nodes downstream of the PLR along the LSP path will be left with stale LSP state until refresh timeout. This condition will not result in any traffic loss. [PR1242558](#)
- With nonstop active routing (NSR), when the rpd restarts on the master Routing Engine, the rpd on the backup Routing Engine might also restart. [PR1282369](#)
- When a make-before-break (MBB) new instance signaling experiences error and before retry is finished, other triggers such as auto bandwidth adjustment timer expiration have to be blocked until MBB finishes. Once the MBB finishes instance switching, a blocked trigger needs to be scheduled, but it should only be triggered after the optimize-adaptive-teardown timer expires. In the affected releases, the blocked trigger is scheduled immediately after instance switching without taking the optimize-adaptive-teardown timer into account. i. As a result, the old instance is torn down before the whole system finishes changing routes using the new instance, which leads to traffic loss. [PR1402382](#)
- When **protocols ldp dual-transport inet-lsr-id** is not the same as router ID, LDP fails to advertise I2circuit label mapping to its neighbor. Thus, I2circuit does not come up properly. [PR1405359](#)
- In LDP over RSVP scenario, clearing RSVP LSP from the CLI, or making path changes which cause RSVP LSP to be re-signaled might lead to rpd memory leak. The memory leak might result in rpd crash when the memory is exhausted. Traffic loss might be seen during the rpd crash. [PR1415774](#)

Network Management and Monitoring

- The `snmpd` daemon leaks memory in `snmpv3` query path and crashes. The issue is caused by a memory leak when the request PDU is dropped by SNMP when **snmp filter-duplicates** is enabled. Each request PDU has a structure pointer for the SNMPv3 security details. This is allocated when the PDU is created or cloned. But while dropping the duplicate requests, the corresponding free for this structure is not done, which causes the memory leak. [PR1392616](#)

Platform and Infrastructure

- In configurations with IRB interfaces, during times of interface deletion (for example, FPC reboot), the Packet Forwarding Engine might log errors stating **nh_ucast_change:291Referenced l2ifl not found**. This condition should be transient, with the system reconverging on the expected state. [PR1054798](#)
- An accuracy issue occurs with three-color policers of both type single rate and two rate in which the policer rate and burst-size combination of the policer accuracy vary. This issue is present starting in Junos OS Release 11.4 on all platforms that use MX Series ASIC. [PR1307882](#)
- Validation for RFC 2544 feature (test start conditions) on MX Series routers is broken in Junos OS Releases 18.3R1 and 18.4R1. An invalid test start condition could lead to an inconsistent state between the Routing Engine and the Packet Forwarding Engine. [PR1396751](#)
- In some cases, the status bit of the RPF next-hop shows as disabled when it should have been enabled. The trigger for the issue is not known yet. [PR1404240](#)

Routing Policy and Firewall Filters

- When **as-path-expand last-as** is configured without the **count** command, the configuration commit fails **set policy-options policy-statement test** then an **as-path-expand last-as root#** commit check error is seen: **Check-out failed for Routing protocols process (/usr/sbin/rpd) without details**. [PR1388159](#)

Routing Protocols

- When only the default routing instance is present, the **show bgp summary** command does not show the BGP establish state. If the BGP state is not an **ESTABLISHED** state, then it shows the states as design (Active, Idle, or Connect). If there is a routing instance configured (apart from master routing-instance inet.0), the BGP ESTABLISH state is showed properly. This issue happens for IPv4 BGP sessions only. On IPv6 we always see all the BGP states as default. [PR600308](#)
- **JTASK_SCHED_SLIP** for `rpd` might be seen while restart routing or ospf protocol disable with scaled BGP routes on MX104 router. [PR1203979](#)
- LDP OSPF are “in sync” state and the reason observed for this is **IGP interface down** with **ldp-synchronization** enabled for OSPF: `user@host> show ospf interface ae100.0` extensive Interface

State Area DR ID BDR ID Nbrs ae100.0 PtToPt 0.0.0.0 0.0.0.0 0.0.0.0 1 Type: P2P, Address: 10.0.60.93, Mask: 255.255.255.252, MTU: 9100, Cost: 1050 Adj count: 1 Hello: 10, Dead: 40, ReXmit: 2, Not Stub Auth type: MD5, Active key ID: 1, Start time: 1970 Jan 1 00:00:00 UTC Protection type: None Topology default (ID 0) -> Cost: 1050 LDP sync state: in sync, for: 00:04:03, reason: IGP interface down config holdtime: infinity. As per the current analysis, **IGP interface down** is observed as the reason because although LDP notified OSPF that LDP synchronization was achieved, OSPF was not able to take note of the LDP synchronization notification, because the OSPF neighbor was not up yet. [PR1256434](#)

- In an IS-IS and IPv6 scenario, rpd might crash when the neighbor router is restarted and cause route churn. [PR1312325](#)
- On all devices running Junos OS enabled with GRES and NSR, if Routing Engine switchover is executed, the BGP peers in the new master Routing Engine might flap due to hold-timer expiry after GRES. [PR1390113](#)
- In a BGP scenario with multipath enabled, if applying import/export policy of IPv6 routes with a IPv4 next-hop to a BGP neighbor, the rpd might crash continuously. [PR1390428](#)
- If an import policy is applied to a BGP neighbor and the policy has indirect IPv4 next-hop for IPv4 and IPv6 routes (IPv6 routes resolved over IPv4), when BGP unresolved route is withdrawn, rpd crash might be seen. [PR1391568](#)
- Policy-based label allocation is not supported for IPV6 prefix. The commit might be successful, but the configuration will not take effect. There is no functional impact. [PR1395040](#)
- The **as-path-group** configuration is limited in scale. With 10,000 lines, scheduler slips are seen, impacting other work the rpd is doing such as protocol keep alives. To avoid the scheduler slips (CPU exhaustion), change how the **as-path-group** is structured. The issue occurs due to two factors: the number of as-path statements under the as-path-group and the wildcards in each of these. [PR1396344](#)
- Memory leak of around 300,000 sessions happens under the following circumstances and when around 2000 flow-spec routes were distributed: 1. remote-operations daemon is running (connect/disconnect of this daemon is causing memory leak and has no relation with this RLI). 2. a) Full BGP configuration is flapped (only in Junos OS Release 18.4) (Deactivate & activate) Full BGP configuration flap means running **delete protocols bgp** and **set protocols bgp**. The issue does not occur if only routes flap. Full configuration flap is not usually done in production network because it resets all BGP routes and routing table contents in the DUT. This is expected in maintenance window, but less likely in customer deployment. b) As a workaround, in Junos OS Releases 18.2X75-D30 and 18.2X75, disable the remote-operations daemon (if not required) by committing the following configuration **set system processes remote-operations disable**. [PR1401914](#)
- Sometimes when a new logical router is configured, a logical router core file might be seen on the system if the kernel is reporting - low memory (this core file is harmless). In subsequent retries by the daemon launcher, logical router gets spawned. [PR1403087](#)
- During NSR initial state replication on a scaled setup there could be cases where although BGP state replication is still ongoing, the BGP task replication might get marked as completed. This is because BGP replication is triggered and controlled through the backup Routing Engine. We advise that you use **show**

bgp replication to confirm if replication has actually completed. This corner-case scenario is valid only on scaled setup and during initial state synchronization. [PR1404470](#)

- In multicast routing scenario using PIM, if configuring static route with qualified-next-hop for multicast source, process rpd might crash. This is because qualified-next-hop points to GF_DLI (Gateway Family Data Links) address which PIM is unable to process, resulting in the crash. [PR1408443](#)
- In BGP with the indirect next-hop scenario, if uRPF or route record is enabled, and then enable BGP multipath, a background job loop might be formed and the CPU utilization of rpd process might be stuck at 100 percent. [PR1414021](#)
- Autotranslation fails when static adj SID is configured with OSPF as IGP. [PR1414612](#)

Subscriber Access Management

- The authd re-uses address too quickly before jdhcpd completely cleanup the old subscriber which flooding error log. The following log message is observed: `jdhcpd: %USER-3-DH_SVC_DUPLICATE_IPADDR_ERR: Failed to add 10.1.128.3 as it is already used by 1815.` [PR1402653](#)

User Interface and Configuration

- The **test configuration** `/config/rescue.conf.gz` fails commit check for the dynamic profile when the subscriber is active. [PR1376689](#)

VPNs

- The multicast VPN MIB is not being properly compiled into the Juniper Networks MIB package bundle. This PR causes `mib-jnx-mvpn.txt` to be included as part of the Juniper Networks MIB set. [PR1394946](#)

SEE ALSO

[New and Changed Features | 69](#)

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

[Known Behavior | 96](#)

[Resolved Issues | 110](#)

[Documentation Updates | 123](#)

[Migration, Upgrade, and Downgrade Instructions | 123](#)

[Product Compatibility | 130](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 19.1R1](#) | 110

This section lists the issues fixed in the Junos OS 19.1R1 Release for MX Series routers.

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

Resolved Issues: 19.1R1

Application Layer Gateways (ALGs)

- DNS requests with EDNS options might be dropped by DNS ALG. [PR1379433](#)

Authentication and Access Control

- MAC move might occur in a DHCP security scenario. [PR1369785](#)
- The dot1xd might crash when dot1xd receives incorrect reply length from the authd. [PR1372421](#)
- IPv4/IPv6 DHCP security client entries will be recorded on TRUSTED ports as well. [PR1390676](#)
- Push-to-JIMS now supports pushing the authenticated entry to all online JIMS servers. [PR1407371](#)

Class of Service (CoS)

- The cosd process might crash during committing configuration change through netconf. [PR1403147](#)

Flow-Based and Packet-Based Processing

- Issues occur with fragmentation and ALG support for Power Mode IPsec. [PR1397742](#)

EVPN

- EVPN type-5 route might be lost if **chained-composite-next-hop** statement is configured. [PR1362222](#)
- Packet drop is seen in EVPN stitching with IRB configured. [PR1363935](#)
- The EVPN implementation does not follow RFC-7432. [PR1367766](#)
- EVPN A/A multihomed PE device occasionally prefers to route to a directly connected prefix using LSPs toward the multihomed peer instead of going directly out of the IRB interface (which is up). [PR1376784](#)
- The RA packets might be sent out without using the configured virtual gateway address. [PR1384574](#)

- EVPN-VXLAN: Flood is not programmed for VTEP interfaces for more than 5 minutes after BGP bounce. [PR1396597](#)
- IPv6 link-local address for virtual-gateway address is marked as duplicate in EVPN. [PR1397925](#)
- When committing a configuration for a VLAN adding to an EVPN instance and an aggregated Ethernet interface, respectively, the newly added VLAN interface count might be zero (0) in that bridge domain. [PR1399371](#)
- EVPN type 2 MAC+IP route is stuck when the route advertisement has two MPLS labels and withdrawal has one label. [PR1399726](#)
- The rpd core file is generated upon Routing Engine switchover with scaled EVPN configuration. [PR1401669](#)
- The rpd crashes due to memory corruption in EVPN. [PR1404351](#)
- EVPN database and bridge mac-table are out of sync after core link flap. [PR1404857](#)
- The rpd might crash on a leaf node when handling withdrawal of the remote or local MAC address in an EVPN-VXLAN scenario. [PR1405681](#)
- The rpd might crash after NSR switchover in a EVPN scenario. [PR1408749](#)

Forwarding and Sampling

- In EVPN A/A scenario with MX or EX acting as PE device, flood next-hops to handle BUM traffic might not get created or miss certain branches when the configuration is performed in a particular sequence. [PR1377749](#)
- LTS subscriber statistics are reported to RADIUS. [PR1383354](#)
- Adjusting **mac-table-size** configuration might cause an l2ald crash. [PR1383665](#)
- The LSI binding for the IPv6 neighbor is missing. [PR1388454](#)
- The filter counter is not written to the accounting file when accounting is enabled on the bridge firewall filter. [PR1392550](#)
- The l2ald process might crash when doing **commit check** for some specific configurations. [PR1395368](#)

General Routing

- We advise migrating from syslog API to Errmsg API: `/src/junos/usr/sbin/mspsmd`. [PR1284654](#)
- MX150: Cannot copy files from the USB flash to Junos OS Virtual Machine. [PR1333201](#)
- Large-scale users logging in and logging out might cause a mgd memory leak. [PR1352504](#)
- Traffic loss might be seen on the new master after interface flap is followed by Routing Engine switchover in a VRRP scenario. [PR1353583](#)
- The packets might be dropped when they go through the MX104 built-in interface. [PR1356657](#)
- The **show chassis ethernet-switch** command output is different on MX10008 routers. [PR1358853](#)

- MX Series BNG does not generate the ESMC/SSM quality level failed SNMP trap alarm. [PR1361430](#)
- The inline J-Flow sampling configuration might cause an FPC crash on MX Series routers. [PR1362887](#)
- MX Series Virtual Chassis: The request to record the VCCP heartbeat state changes in syslog by default. [PR1363565](#)
- FPM board status is missing in the SNMP MIB walk result. [PR1364246](#)
- The netproxy service client component fails to restart after issuing the **request vmhost reboot** command. [PR1365664](#)
- The following errors are seen in the syslog: **LOG : Err] Failed to allocate 2 jnh-dwords for encap-ptr(ether-da)!,LOG: Err] gen_encap_common: jnh-alloc failed! 8** [PR1366811](#)
- When you configure vrrp delegate-processing with tomcat enabled, the Packet Forwarding Engine dropped vrrp packets and count sw error. [PR1369503](#)
- MPC5E restarted at **trinity_pio_io_func, pio_read_u32, xqchip_read_u32, xqchip_issu_disable_q_stats, qchip_issu_disable_q_stats, issu_asic_prepare (pfe_idx=0 '\000')** at **../../../../src/pfe/common/applications/issu/jam/issu_jam_npc_pfe.c:65** [PR1369635](#)
- Image installation on SD fails with the following error: **Unable to read reply from software add command to re1; error 1.** [PR1372877](#)
- Core file is generated in ifinfo at **pif_af_fe_info pif_af_ifd** when displaying the af interface information. [PR1373436](#)
- LDP convergence delay might be seen after a IGP metric change with the **bgp-igp-both-ribs** statement configured. [PR1373855](#)
- The filter service might fail to get installed for the subscriber in a scaled BBE scenario. [PR1374248](#)
- A few L2BSA subscribers might be stuck in init, terminating, or terminated state after the previous logout. [PR1375070](#)
- SFB and PDM/PSU-related information is missing in jnxBoxAnatomy MIB on high-end MX Series routers. (MX2010/2020). [PR1375242](#)
- The bbe-smgd core file might be seen after doing GRES. [PR1376045](#)
- MS-MPC might have performance degradation under scaled fragmented packets. [PR1376060](#)
- Interface optic output power is not zero when the port has been disabled. [PR1376574](#)
- CI: Not generating Power Supply failed trap. [PR1376612](#)
- After NAT64 router (with MS-MPC) translates an IPv6 fragment to an IPv4 fragment, router is not inserting the correct value in the identification field of the IPv4 header. [PR1378818](#)
- The bbe-smgd process generates repeated core files and stops running as a result of long-term session database shared memory corruption. [PR1388867](#)
- Traffic might be discarded without notification when CoS configuration is changed on a PS interface. [PR1379530](#)

- Protocol adjacency might flap and FPC might reboot if jlock hog happens. [PR1379657](#)
- MSQQ error logs and potential MPC traffic impact are seen when the physical interface link goes down. [PR1380183](#)
- The pfe_disable action should also disable the logical interfaces belonging to the affected Packet Forwarding Engine. [PR1380784](#)
- Encryption and decryption is not happening, because the Packet Forwarding Engine discards it while testing that group-vpn member was established using the authentication-method preshared key ascii-text. [PR1381316](#)
- Traffic might be discarded without notification that is caused by FPC offline in MC-LAG scenario. [PR1381446](#)
- In MX3ru for Junos OS Release 18.3R1, unified ISSU will fail if QSA is plugged in. [PR1382126](#)
- The MPC6E might crash while fetching PMC device states. [PR1382182](#)
- High CPU utilization is seen for chassisd on bsys, ~20 percent st steady state. [PR1383335](#)
- The configuration configured through the NETCONF session might fail. [PR1383567](#)
- MBFD flaps because clksync congests the scheduler for 100 ms. [PR1384473](#)
- The rpd generates a core file at `krt_table_rtbit_q_handler` , `krt_q_flush (startp=0xcca2c500, endp=0xcca2e9d0, isflash=0, todo=0x7ffffffe204),rtbit_free (rtbh=0x4145540)`. [PR1385005](#)
- The MPLS packets with more than eight labels will not be processed by J-Flow. [PR1385790](#)
- The vFPC CPU is running very high on vMX. [PR1385853](#)
- The device with more than five IP addresses configured in the DHCP server-group goes into amnesiac mode after reboot. [PR1385902](#)
- In subscriber management environment DHCP Subscriber might get stuck in terminated state. [PR1386662](#)
- In case an LSP is locally configured without an explicit path, the ERO object remains empty in the PCRpt generated by PCC. [PR1386935](#)
- Uninitialized EDMEM[0x400094] Read (0x6db6db6d6db6db6d) logs are seen with sampling applied to a subscriber with routing-service applied. [PR1386948](#)
- The rpd might crash when traceoptions are enabled. [PR1387050](#)
- On MX2000 routers, the backup CB's chassis environment status shows up as "Testing" even after the backup CB becomes online by removal or insert operation. [PR1387130](#)
- The bbe-smgd process might crash when two subscribers log in with the same framed-route prefix and preference values. [PR1387690](#)
- Some SFBs might go down when one of the PSMs in the chassis generates a bad output voltage that is out-of-range. [PR1387737](#)

- FPC core file is seen at sensor_export_time_exceed_limit agent_health_monitor_data_reap when **Jinsight** is configured. [PR1388112](#)
- Psec IKE keys are not cleared when delete or clear notification is received from peer on GRES-enabled DUT. [PR1388290](#)
- Fabric drops might be seen if using a newer generation of MPC with SFB2. [PR1388780](#)
- Incorrect value for flow packets or octets fields might be seen in an inline J-Flow scenario, [PR1389145](#)
- IGMP group threshold exceed log message prints an incorrect demux logical interface. [PR1389457](#)
- MX204: Excluding the **speed** CLI option under the interface level. [PR1389918](#)
- The jnxFruState might show incorrect PIC state after replacing an MPC with another MPC with less number of PICs. [PR1390016](#)
- Traffic destined to VRRP VIP gets dropped because the filter is not updated to the related logical interface. [PR1390367](#)
- The **delete chassis redundancy** command with routing-options nonstop-routing is not giving a commit warning. [PR1390575](#)
- Delay in CLI output with second or more **show subscriber <> extensive** queries when the first session is sitting at -(more)- prompt displaying **show subscribers extensive** command output. [PR1390762](#)
- Trailing chars are seen in GNMI get API reply. [PR1390967](#)
- All the BBE and ESSM subscriber sessions might be lost after GRES or unified ISSU. [PR1391409](#)
- The **routing-engine-power-off-button-disable** statement does not work on MX204 and MX10003 routers. [PR1391548](#)
- The bbe-smgd process might crash after committing configuration changes. [PR1391562](#)
- The bbe-smgd process might crash in a corner case if family inet6 is used in the dynamic profile. [PR1391845](#)
- On MX2000, fans start spinning at high speed upon inserting previously offlined FPC. [PR1393256](#)
- Third-generation FPC reboot loop is caused because of having internal intf issues. [PR1393643](#)
- Junos OS enhancement configuration statement added to modify mcontrol watchdog timeout. [PR1393716](#)
- If FPGA on the new master CB has a specific hardware failure, the chassis might keep crashing after GRES switchover. [PR1393884](#)
- Expected entries like "UI_COMMIT_PROGRESS" are not getting populated while checking with Junos OS script session for obtaining the syslog output. [PR1394780](#)
- MPC7, MPC8, and MPC9 might not boot in the MX Series Virtual Chassis. [PR1396268](#)
- Adding IRB to bridge-domain with PS interface causes a kernel crash. [PR1396772](#)
- The MS-MPC might generate a core file when mspmand receives a non-synchronized packet of TCP. [PR1396785](#)

- A smid process memory leak occurs, and it does not come down from 100 percent. [PR1397643](#)
- PFT MX10008: Inline-services enabling the **Flex-Flow-Sizing** take more than 12 minutes to move to steady state. [PR1397767](#)
- The **show system errors active** command is not showing the error for MPC3E next-generation HQoS. [PR1398084](#)
- Kernel core file is generated on vMX. [PR1398320](#)
- MPLSoUDP tunnels do not come up on interface route - dyn_tunnel_fwd_route_eligible - because next-hop type is configured as interface. [PR1398362](#)
- High jsd or na-grpcd CPU usage might be seen even if JET or JTI is not used. [PR1398398](#)
- IPsec tunnel cannot be established, because the tunnel SA and rule are not installed in the PIC. [PR1398849](#)
- The bbe-smgd process might crash when executing the **show pppoe lockout** command. [PR1398873](#)
- Wrong timestamp is displayed in the jvision collector log file. [PR1399829](#)
- ARP refresh functionality might fail in an EVPN scenario. [PR1399873](#)
- JET/PRPD incompatibility for the rib_service.proto field RouteGateway.weight occurs from Junos OS Release 18.4R1 to Release 18.4R2 and onward. [PR1400563](#)
- The mgd-api crashes due to memory leak. [PR1400597](#)
- Only one Packet Forwarding Engine could be disabled on FPC with multiple Packet Forwarding Engines in error/wedge condition. [PR1400716](#)
- The authd might crash when issuing the **show network-access requests pending** command during the authd restarting. [PR1401249](#)
- The **show | compare** output on global group changes loses the diff context after a rollback or “load update” is performed. [PR1401505](#)
- The subscriber route installation fails because some interface states are not properly installed. [PR1401506](#)
- FPC core files are generated due to a corner case scenario (race condition between RPF, IP flow). [PR1401808](#)
- JET authentication does not work for usernames and passwords of certain lengths. [PR1401854](#)
- Traffic loss is seen for IGMP subscribers after GRES. [PR1402342](#)
- The MPC might crash due to the CPU hogging by dfw thread. [PR1402345](#)
- Some error logs might be seen on FPC when reading attempt from uninitialized memory location. [PR1402484](#)
- FPC might crash after you offline or online MIC-3D-16CHE1-T1-CE-H. [PR1402563](#)
- DHCP subscriber cannot reconnect over dynamic VLAN demux interfaces because of RPF check failure. [PR1402674](#)
- Host outbound traffic might be dropped on MPC7, MPC8, and MPC9 [PR1402834](#)

- Observed rpd core files when a few colored LSPs are changed to uncolored LSPs. The cores are at <<< **#0 tag_cmp_tag (tag1=0x0, tag_label1=0x0, tag2=0x98b6628, tag_label2=0x98b6644)** at `../../../../src/junos/usr/sbin/rpd/lib/mps/label_mgr/core/mps_label.c:473 473` if `(tag1->tagt_mtu != tag2->tagt_mtu)` >>> [PR1403208](#)
- Reported Log Variance might be incorrect if the PTP profile is changed from G.8275.2 to SMPTE or another multicast IP profile. [PR1403219](#)
- Smg-service might become unresponsive. [PR1403480](#)
- The time synchronization through PTPoE might not work when Enhanced Subscriber Management is enabled on MX Series routers. [PR1404002](#)
- The FPC might crash in a CoS scenario. [PR1404325](#)
- The repd continues to generate core files on VC-Bm when there are too many IPv6 addresses on one session. [PR1404358](#)
- The **targeted-broadcast** statement does not work on the IRB interface. [PR1404442](#)
- Configuration load override or load replace resets ANCP neighbors. [PR1405318](#)
- NAT64 translation issues of ICMPv6 packet-too-big message occur with MS-MPC/MS-PIC. [PR1405882](#)
- Fabric performance drop is seen on MPC7, MPC8, MPC9E, and SFB2-based MX2000 routers. [PR1406030](#)
- Traffic impact might be seen if **auto-bandwidth** is configured for RSVP LSPs. [PR1406822](#)
- New CLI option is introduced to display DF and MLR in split format. [PR1406884](#)
- Layer 2 VPN will flap repeatedly after link up between PE and CE devices under "asynchronous-notification" and "some types of MICs" conditions. [PR1407345](#)
- NPC core files are generated after daemon restart in **#0 jnh_get_oif_nh (ifd=0x51a51a80, ifl=0x6aeb52e0, family_mtu=0, max_mpls_labels=0 '\000', pad_ge_frame_check=< optimized out>, ret_jnh=0x483a54a8)** at `../../../../src/pfe/common/pfe-arch/trinity/toolkits/jnh/jnh_if.c:15248`. [PR1407765](#)
- Ephemeral database might get stuck during commit. [PR1407924](#)
- Traffic forwarding fails when crossing VCF members. [PR1408058](#)
- Alarm mismatch in total memory is detected after running the **reboot vmhost both** command. [PR1408480](#)
- TFTP of MPC line cards images fails when performing unified ISSU. [PR1408558](#)
- Python script might stop working due to **Too many open files** error. [PR1408936](#)
- interface-set meta-data needs to include the CoS TCP names in order to aid collector reconciliation with queue-stats data. [PR1409625](#)
- FPC might generate core files during next-hop change due to FPC reboot or interface flap when using MPLS inline J-Flow. [PR1409807](#)
- When using SFP+, the interface optic output might be non-zero even when the interface has been disabled. [PR1410465](#)

- Traffic loss might be seen on MPC8E and MPC9E after requesting one of the SFB2s to go offline/online. [PR1410813](#)
- Kernel replication failure and vmcore are seen because **add IPv6 route prefix** operation is not supported with the next-hop to be ATM interface. [PR1411376](#)
- MX10003: The rpd crash with switchover-on-routing-crash does not trigger a Routing Engine switchover and the rpd on the master Routing Engine goes into STOP state. [PR1412322](#)
- During unified ISSU from Junos OS Release 16.1R4-S11.1 to Junos OS Release 18.2R2-S1.2, CoS GENCFG write failures are observed: [**COS(cos_rewrite_do_pre_bind_add_action:676): Binding of table 44226 to ifl 1073744636 failed, table already bound to ifl**]. [PR1413297](#)
- MPC10E line card will not power up in old MidPlane MX chassis when using Junos OS Release 19.1R1. [PR1413373](#)
- Broken support of [family inet6 filter] on the ATM interface. [PR1413663](#)
- The bbe-smgd process might have memory leak while running the **show system subscriber-management route route-type <> routing-instance <>** command. [PR1415922](#)
- In the scenario where the MX and the peer both try to bring an IPsec tunnel up but the peer side does not answer the MX requests, we can bring the peer initiated tunnel down. [PR1420293](#)

Infrastructure

- The error of **jlaunchd: disk-monitoring is thrashing, not restarted** might be seen. [PR1380032](#)

Interfaces and Chassis

- In case of MPLS, DMR packets are sent with different MPLS expiration bits if the MX Series router receives CFM DMM packets with varying expiration values on the MPLS header. [PR1365709](#)
- Constant dcpfe process crash might be seen if using an unsupported GRE interface configuration. [PR1369757](#)
- The jpppd process might crash if the EPD value contains a format specifier. [PR1384137](#)
- DCD core file can be seen after FPC restart if **channelized interfaces** are configured. [PR1387962](#)
- All DPCs might crash while adding or deleting a logical interface from the aggregated Ethernet bundle. [PR1389206](#)
- The interface-control process thrashes and dcd does not restart after adding an invalid demux interface to the configuration. [PR1389461](#)
- Decoupling of Layer 2 logical interface configuration from bridge-domain or EVPN configuration. [PR1390823](#)
- Interim accounting updates might not be sent for subscribers after Junos OS selective update. [PR1391011](#)
- A dcd memory leak might be seen when committing configuration change on static route tag. [PR1391323](#)
- Error message might be seen if GR interface is configured. [PR1393676](#)

- DCD crashes on deleting the sub interface from VPLS routing-instance when the same sub interface is also part of mesh-group. [PR1395620](#)
- The **MIC Error code: 0x1b0002** alarm might not be cleared for MIC on MPC6 when the voltage has returned to normal. [PR1398301](#)
- The backup Routing Engine might get stuck in amnesiac mode after reboot. [PR1398445](#)
- All dcd operations might be blocked if profile-db is corrupt. [PR1399184](#)
- Certain otn-options cause interface flapping during commit. [PR1402122](#)
- Subscriber might not be able to access the device due to the conflicted assigned address. [PR1405055](#)
- The cfmd might fail to start after it is restarted. [PR1406165](#)
- The aaa-options configuration statement for PPPoE subscribers does not work on the MX80 and MX104 routers. [PR1410079](#)

Layer 2 Features

- The unicast traffic from IRB interface toward LSI might be dropped due to Packet Forwarding Engine mismatch at egress processing. [PR1381580](#)
- Flow label is still used by ingress PE though the egress PE is not configured/supporting for Flow label in a VPLS multihomed Scenario. [PR1393447](#)
- In a Layer 2 domain (for example, bridge-domain, VPLS), there is unexpected flooding of unicast traffic at approximately every 40 seconds toward all local CE-facing interfaces. [PR1406807](#)

Layer 2 Ethernet Services

- The subscriber's authentication might fail when the link-layer address that is encoded in the DHCPv6 DUID is different from the actual link-layer hardware address. [PR1390422](#)
- The SNMP query on LACP interface might lead to lacpd crash. [PR1391545](#)
- Log messages `dot1xd[]: task_connect: task ESP CLIENT:.... Connection refused` might be reported in Junos OS Release 17.4 or later. [PR1407775](#)

MPLS

- The rpd might crash on the backup Routing Engine after switchover. [PR1382249](#)
- MPLS LSP will remain in the down state due to routing loop detection after flapping link between PE router and egress PE router. [PR1384929](#)
- Configured bandwidth 0 does not get applied on the RSVP interface. [PR1387277](#)
- The bypass LSP might pass through an unexpected path that includes the same SRLG as the protected TE link that is down. [PR1387497](#)
- The rpd process might keep crashing repeatedly if the LSP destination address is set to be 0.0.0.0. [PR1397018](#)

- The rpd might crash when the LDP route with indirect next-hop is deleted. [PR1398876](#)
- A single-hop bypass LSP might not be used for traffic when both transit chaining mode and sensor-based statistics are used. [PR1401152](#)
- Resources might be reserved for stale RSVP LSP when RSVP is disabled on the interface. [PR1410972](#)
- LDP crash is caused by an `ldp_label_bind_route` assert condition. [PR1413231](#)
- LDP native IPv6 loopback remains in inet6.3 after removing the IPv6 address from the core interface. [PR1414965](#)

Platform and Infrastructure

- MQCHIP CPQ block should report major alarm. [PR1276132](#)
- Some line cards might crash in a subscriber scenario enabled with distributed IGMP. [PR1355334](#)
- The FPC might crash continuously when the filters in the same filter list refer to a same nested filter [PR1357531](#)
- The kernel and ksyncd core files are generated after dual cb flap at `rt_nhfind_params: rt_nhfind()` found a next-hop different from that on the master 30326. [PR1372875](#)
- The traffic traversing an IRB interface might not be tagged with a VLAN if the packets go through an additional routing instance. [PR1377526](#)
- IPv6 ping might fail for spine node in a EVPN scenario. [PR1380590](#)
- Packet drops on interface occur if the **gether-options loopback** statement is configured. [PR1380746](#)
- The dfwd might crash with **DFWD_TRASHED_RED_ZONE** log messages. [PR1380798](#)
- Traffic loss is seen in Layer 2 VPN with GRE tunnel. [PR1381740](#)
- MAC learning might get stuck on MX Series routers with DPC and MPC. [PR1383233](#)
- jlock hog is reported at restart routing. [PR1389809](#)
- Individual command authorization might cause mgd crash. [PR1389944](#)
- Traffic is being dropped when passing through MS-DPC to MPC. [PR1390541](#)
- The RADIUS authentication does not work through management-instance for IPv6 family. [PR1391160](#)
- The lockout-period might not work for the user being locked out. [PR1393839](#)
- RVT interface might start flapping. [PR1399102](#)
- In a scaled scenario (500 TWAMP control sessions and 500 TWAMP test sessions), a few TWAMP connections might fail to establish. [PR1399547](#)
- Syslog error messages: `[LOG: Err] COS_HALP(cos_halp_get_fabric_stats_per_pfe:3211): pfe_id 0 cchip 0[LOG: Err] COS_HALP(cos_halp_get_fabric_stats_per_pfe:3272): No PFE found for pfe_id_start 0.` [PR1402377](#)
- MAP-E some ICMP types cannot be encapsulated/decapsulated on SI interface. [PR1404239](#)

- When a non-root user tries to archive the **var/log**, some files are missing if a **cscript.log** file exists. [PR1405903](#)
- Abnormal queue-depth counters appear in **show interface queue** command output on interfaces associated to XM2 and 3. [PR1406848](#)
- Ipv6 drops due to **output trunk vlan lookup failed**. [PR1407200](#)

Routing Policy and Firewall Filters

- The **set metric multiplier offset** might overflow or underflow. [PR1349462](#)
- The rpd process might crash if **then next-hop** is configured for the LDP export policy. [PR1388156](#)
- The rpd process might crash when **routing-options flow** configuration is removed. [PR1409672](#)

Routing Protocols

- BGP might not advertise routes on the existing BGP peer after adding a Layer 3 VPN instance. [PR1237006](#)
- Migrate from syslog API to Errmsg API: **/src/junos/usr.sbin/ppmd**. [PR1284621](#)
- The BGP session might be stuck with high BGP OutQ value after GRES on both sides. [PR1323306](#)
- The VRF static route might not be exported when **route-distinguisher-id** is used on RR in a BGP Layer 3 VPN scenario. [PR1341720](#)
- The dynamic next-hop template cache does not shrink when the application frees the next-hop template and there are surplus templates in cache. [PR1346984](#)
- vFPC might continuously crash on vMX platform. [PR1364624](#)
- Ukern memory leak and core crash are seen in BGP environment. [PR1366823](#)
- The static route might persist even after its BFD session goes down. [PR1385380](#)
- The rpd might crash after issuing the **show route detail** operational command for RIP route. [PR1386873](#)
- Penultimate-hop router does not install BGP LU label, causing traffic to be discarded without notification. [PR1387746](#)
- IGMPv3/MLD membership requests might not work normally. [PR1389119](#)
- Unexpected packet loss might be seen for some multicast groups during failure recovery with both MoFRR and PIM automatic MBB join load-balancing features enabled. [PR1389120](#)
- FPC might crash when BGP multipath is configured with protection. [PR1389379](#)
- BGP IPv6 routes with IPv4 next-hop causes the rpd to crash. [PR1389557](#)
- All the BGP sessions will flap after switchover. [PR1391084](#)
- The ppmd on the Routing Engine might run with high CPU utilization after a Routing Engine switchover. [PR1392704](#)
- The rpd core files are generated on the backup Routing Engine during neighborship flap when using an authentication-key with more than 20 characters. [PR1394082](#)

- The rpd process might crash when **rp-register-policy** is configured with more than 511 terms. [PR1394259](#)
- The best and the second-best routes might have the same weight value if BGP PIC is enabled. [PR1395098](#)
- DMZ LINK BANDWIDTH - not able to aggregate bandwidth, when applying the policy. [PR1398000](#)
- The rpd soft core might be seen when Layer 2 VPN is used. [PR1398685](#)
- The rpd might crash in BGP setup with NSR enabled. [PR1398700](#)
- The rpd might crash when BGP **add-path send** is configured and NSR is enabled. [PR1401948](#)
- BGP router on the same broadcast subnet with its neighbors might cause IPv6 routing issue on the neighbor from other vendors. [PR1402255](#)
- EVPN multihoming MAC might not be installed by the remote PE device. [PR1403881](#)
- Memory leaks when labeled-isis transit routes are created as chain composite next-hop. [PR1404134](#)
- Extended traffic loss might be seen after link recovery when source-packet-routing is used on OSPF P2P links. [PR1406440](#)
- SBFD failure occurs with a special IP address like 127.0.0.1 under interface lo0. [PR1406631](#)
- The rpd crashes with BGP functions `bgp_peer_tcpwriteerror_gracefully`. [PR1410553](#)

Services Applications

- L2TP subscribers might be stuck in init state in a corner case. [PR1391847](#)
- The spd might crash when **any-ip** is configured in the 'from' clause of the NAT rule with the static translation type. [PR1391928](#)
- IP ToS bits are not copied to the outer IPsec header. [PR1398242](#)
- Invalid Layer 4 checksum might be observed on IPv4 packets generated by NAT64 with MS-DPC after translating fragmented IPv6 UDP/TCP packets. [PR1398542](#)
- The ICMPv6 packet with embedded IPv6 fragment might not be translated correctly to an IPv4 ICMP packet in a NAT64 with MS-DPC deployment. [PR1402450](#)
- Inconsistent content might be observed to the access line information between ICRQ and PPPoE message. [PR1404259](#)
- The stale si- logical interface might be seen when L2TP subscribers with duplicated prefixes or framed-route log in. [PR1406179](#)
- The kmd process might crash on MX/ACX platforms when IKEv2 is used. [PR1408974](#)

Subscriber Access Management

- The subscribers might be stuck in terminating state if RADIUS redirect is used. [PR1376265](#)
- Multiple IPv6 IANA addresses are assigned for one session in a IPv6 PD binding failure scenarios. [PR1384889](#)

- Dual-stacked DHCPv6-PD client connection terminated after commit when RADIUS address assignment is not defined within the range of a local pool. [PR1401839](#)
- The authd crash might be seen due to a memory corruption issue. [PR1402012](#)
- Adding a firewall filter service through the **test aaa** command causes a crash in dfwd. [PR1402051](#)
- JSRC used RADIUS service accounting protocol instead of JSRC for SRC installed service. [PR1403835](#)
- Continuous log message **authd[18454]: %DAEMON-3-LI: liPollTimerExpired returned 0** is seen. [PR1407923](#)

User Interface and Configuration

- The **show configuration** and **rollback compare** commands are causing high CPU usage. [PR1407848](#)

VPNs

- The receivers belonging to a routing instance might not receive multicast traffic in an Extranet next-generation MVPN scenario. [PR1372613](#)
- The **accept-remote-source** statement configured on the core interface might cause traffic outage. [PR1375716](#)
- High rpd CPU utilization on the backup Routing Engine might be observed in an MVPN with NSR scenario. [PR1392792](#)
- The rpd process crashes when the LSP template for a provider tunnel is changed. [PR1395353](#)
- Downstream interface is not removed from multicast route after getting PIM prune. [PR1398458](#)
- Routes with multiple communities might be rejected in an inter-AS next-generation MVPN scenario. [PR1405182](#)
- With rosen MVPN configuration with data-mdt, the **show pim mdt data-mdt-limit instance <interface name>** with family option causes high CPU usage of the rpd. [PR1405887](#)

SEE ALSO

[New and Changed Features | 69](#)

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

[Known Behavior | 96](#)

[Known Issues | 99](#)

[Documentation Updates | 123](#)

[Migration, Upgrade, and Downgrade Instructions | 123](#)

[Product Compatibility | 130](#)

Documentation Updates

IN THIS SECTION

- [Spanning Tree Protocol User Guide | 123](#)

This section lists the errata and changes in Junos OS Release 19.1R1 documentation for MX Series.

Spanning Tree Protocol User Guide

- Documentation on configuring Layer 2 Protocol Tunneling (L2PT) for spanning-tree protocols on MX Series and ACX Series routers has been removed from the [Spanning-Tree Protocols User Guide](#) and merged into [Layer 2 Protocol Tunneling](#) in the [Ethernet Switching User Guide](#).

SEE ALSO

[New and Changed Features | 69](#)

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

[Known Behavior | 96](#)

[Known Issues | 99](#)

[Resolved Issues | 110](#)

[Migration, Upgrade, and Downgrade Instructions | 123](#)

[Product Compatibility | 130](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading to Release 19.1 | 124](#)
- [Procedure to Upgrade to FreeBSD 11.x based Junos OS | 125](#)
- [Procedure to Upgrade to FreeBSD 6.x based Junos OS | 127](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 129](#)

- Upgrading a Router with Redundant Routing Engines | 129
- Downgrading from Release 19.1 | 130

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

Starting in Junos OS 18.3R1 release, FreeBSD 11.x is the underlying OS for all Junos OS platforms which were previously running on FreeBSD 10.x based Junos OS. FreeBSD 11.x does not introduce any new Junos OS related modifications or features but is the latest version of FreeBSD.

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

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

Basic Procedure for Upgrading to Release 19.1

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

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

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

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

Procedure to Upgrade to FreeBSD 11.x based Junos OS

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

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

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

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

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-32-19.1R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-64-19.1R1.9-signed.tgz
```

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-32-19.1R1.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-64-19.1R1.9-limited.tgz
```

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

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

Do not use the **validate** option while upgrading from Junos OS (FreeBSD 6.x) to Junos OS (FreeBSD 11.x). This is because programs in the **junos-upgrade-x** package are built based on FreeBSD 11.x, and Junos OS (FreeBSD 6.x) would not be able to run these programs. You must run the **no-validate** option. The **no-validate** statement disables the validation procedure and allows you to use an import policy instead.

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

Rebooting occurs only if the upgrade is successful.

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

NOTE: After you install a Junos OS Release 19.1 **jinstall** package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add no-validate** command and specify the **jinstall** package that corresponds to the previously installed software.

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

Procedure to Upgrade to FreeBSD 6.x based Junos OS

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

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

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/>
2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.
4. Select the **Software** tab.
5. In the **Install Package** section of the **Software** tab, select the software package for the release.

6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **jinstall** package on the routing platform.

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

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

```
user@host> request system software add validate reboot source/jinstall-ppc-19.1R1.9-signed.tgz
```

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

```
user@host> request system software add validate reboot
source/jinstall-ppc-19.1R1.9-limited-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 19.1 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1, 17.2, and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

Upgrading a Router with Redundant Routing Engines

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

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

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

Downgrading from Release 19.1

To downgrade from Release 19.1 to another supported release, follow the procedure for upgrading, but replace the 19.1 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

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

SEE ALSO

New and Changed Features		69
Changes in Behavior and Syntax		90
Known Behavior		96
Known Issues		99
Resolved Issues		110
Documentation Updates		123
Product Compatibility		130

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility](#) | [130](#)

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://apps.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 69
Changes in Behavior and Syntax 90
Known Behavior 96
Known Issues 99
Resolved Issues 110
Documentation Updates 123
Migration, Upgrade, and Downgrade Instructions 123

Junos OS Release Notes for NFX Series

IN THIS SECTION

- [New and Changed Features | 132](#)
- [Changes in Behavior and Syntax | 134](#)
- [Known Behavior | 135](#)
- [Known Issues | 136](#)
- [Resolved Issues | 137](#)
- [Documentation Updates | 138](#)
- [Migration, Upgrade, and Downgrade Instructions | 138](#)
- [Product Compatibility | 141](#)

These release notes accompany Junos OS Release 19.1R1 for the NFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- [What's New in Release 19.1R1](#) | 132

This section describes the new features and enhancements to existing features in Junos OS Release 19.1R1 for NFX Series devices.

What's New in Release 19.1R1

Hardware

- **xDSL SFP modules (NFX250 NextGen)**—Starting in Junos OS Release 19.1R1, NFX250 NextGen devices support xDSL SFPs. The xDSL SFPs are supported on the SFP and SFP+ ports on the devices. Note that the xDSL SFPs are not supported on the extension modules. The xDSL SFP supports ADSL2/2+ and VDSL2.

[See [ADSL2 and ADSL2+ Interfaces on NFX250 \(NextGen\) Devices](#).]

[See [ADSL2 and ADSL2+ Interfaces on NFX250 Devices](#).]

[See [VDSL2 Interfaces on NFX250 Devices](#).]

Application Security

- **Application Quality of Experience (AppQoE) on NFX150 dual CPE deployments**—Starting in Junos OS Release 19.1R1, you can configure Application Quality of Experience (AppQoE) on NFX150 dual CPE deployments. AppQoE effectively prioritizes, segregates, and routes business-critical applications traffic without compromising performance or availability.

[See [Application Quality of Experience on NFX Devices](#).]

- **AppQoE scaling support (NFX250)**—Starting in Junos OS Release 19.1R1, Application Quality of Experience (AppQoE) enforces the configuration limit for overlay paths, metric profiles, probe parameters, and SLA rules per profile when you configure application-specific SLA rules and associate the SLA rules to an APBR profile. If you configure more parameters than the allowed limit, an error message is displayed after you commit the configuration.

[See [Application Quality of Experience on NFX Devices.](#)]

Architecture

- **Reoptimized architecture support (NFX250 NextGen)**—Starting in Junos OS Release 19.1R1, NFX250 devices support a reoptimized architecture, which enables you to use the Junos Control Plane (JCP) as the single point of management to manage all the components.

NOTE: For documentation purposes, the NFX250 devices that use this architecture are referred to as NFX250 NextGen.

Key components in the software include the JCP, Juniper Device Manager (JDM), Layer 2 dataplane, Layer 3 dataplane, and virtualized network functions (VNFs). The JDM functions in the background. Users cannot access the JDM directly.

[See [How to Configure NFX250 \(NextGen\).](#)]

Firewall User Authentication

- **Firewall user authentication (NFX150)**—Starting in Junos OS Release 19.1R1, pass-through firewall user authentication is supported on NFX150 devices. Pass-through authentication restricts users who attempt to access a resource in another zone using FTP, Telnet, HTTP, or HTTPS. If the traffic matches a security policy that specifies pass-through authentication, the user is required to provide login information. The device validates the username and password against the information stored in the local database or on an external authentication server. The device supports the external authentication servers RADIUS, LDAP, and SecurID.

[See [Integrated User Firewall.](#)]

High Availability

Performance modes

- **Performance modes (NFX150 and NFX250 NextGen)**—Starting in Junos OS Release 19.1R1, NFX150 and NFX250 NextGen devices provide the following three performance modes:
 - **Throughput mode**—Provides maximum resources (CPU and memory) for Junos software and remaining resources, if any, for third-party VNFs. The default mode is throughput mode.
 - **Hybrid mode**—Provides a balanced distribution of resources between the Junos software and third-party VNFs.
 - **Compute mode**—Provides minimal resources for Junos software and maximum resources for third-party VNFs.

[See [NFX150 Feature Overview.](#)]

[See [NFX250 NextGen Overview](#).]

Wireless WAN

- **LTE support in dual CPE deployments (NFX150)**—Starting in Junos OS Release 19.1R1, you can provide a backup WAN connection by configuring LTE modules on a pair of NFX150 devices operating in cluster mode.

[See [Configuring the LTE Module on NFX Devices](#).]

SEE ALSO

[Changes in Behavior and Syntax | 134](#)

[Known Behavior | 135](#)

[Known Issues | 136](#)

[Resolved Issues | 137](#)

[Documentation Updates | 138](#)

[Migration, Upgrade, and Downgrade Instructions | 138](#)

[Product Compatibility | 141](#)

Changes in Behavior and Syntax

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 19.1R1 for the NFX Series.

SEE ALSO

[New and Changed Features | 132](#)

[Known Behavior | 135](#)

[Known Issues | 136](#)

[Resolved Issues | 137](#)

[Documentation Updates | 138](#)

[Migration, Upgrade, and Downgrade Instructions | 138](#)

[Product Compatibility | 141](#)

Known Behavior

IN THIS SECTION

- [High Availability \(HA\) | 135](#)

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 19.1R1 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.

High Availability (HA)

- On NFX150 HA topology, when one of the nodes is down or rebooting, any configuration commit on the peer active node triggers a reboot of the active node. This leads to loss of network connectivity until any one of the nodes in the HA topology becomes active. [PR1427550](#)

SEE ALSO

[New and Changed Features | 132](#)

[Changes in Behavior and Syntax | 134](#)

[Known Issues | 136](#)

[Resolved Issues | 137](#)

[Documentation Updates | 138](#)

[Migration, Upgrade, and Downgrade Instructions | 138](#)

[Product Compatibility | 141](#)

Known Issues

IN THIS SECTION

- [Security | 136](#)
- [Performance Modes | 136](#)

This section lists the known issues in hardware and software in Junos OS Release 19.1R1 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.

Security

- Starting in Junos OS Release 19.1R1, the TCP and ICMP RPM probes take the best effort queue of the outgoing interface instead of the network control queue on NFX150 and NFX250 (NG) devices. As a workaround, configure a DSCP value such as nc1, to make the RPM probes take the network control queue. [PR1329643](#)
- When you commit after adding or deleting class-of-service (CoS) configurations for interfaces on NFX150 and NFX250 (NG) devices, **NFX3/ACX5448:LIBCOS_COS_TVP_FC_INFO_NOT_FOUND: Forwarding-class information not specified** is displayed. As a workaround, configure **set system syslog user * match "!(LIBCOS_COS_TVP_FC_INFO_NOT_FOUND: Forwarding-class information not specified)".** [PR1376665](#)

Performance Modes

- Starting in Junos OS Release 19.1R1, NFX150 and NFX250 NextGen devices can operate in three modes with separate allocation of system resources. By default, all resources are used by system components. This might prevent from instantiating the VNFs that are configured on the device. As a workaround, change the mode of the device to compute mode by using the command, **request vmhost mode compute.** [PR1426436](#)

SEE ALSO

[New and Changed Features | 132](#)

Changes in Behavior and Syntax	134
Known Behavior	135
Resolved Issues	137
Documentation Updates	138
Migration, Upgrade, and Downgrade Instructions	138
Product Compatibility	141

Resolved Issues

IN THIS SECTION

- Resolved Issues: 19.1R1 | 137

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

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

Resolved Issues: 19.1R1

NFX250

- Junos Device Manager (JDM) depends on the libvirtd daemon to manage the guest VMs through CLI. On NFX250 devices running Junos OS Release 19.1R1, the libvirtd daemon is inactive and the vjunos VM start up fails. This results in inband connectivity failure, guest VMs fails to start, and the console is hung. [PR1314945](#)

NFX150

- On NFX150 devices running Junos OS Release 19.1R1, software upgrade does not delete all images from the previous installation. This occupies 1GB of storage per upgrade and leads to depletion of storage after several upgrades. [PR1408061](#)

SEE ALSO

New and Changed Features 132
Changes in Behavior and Syntax 134
Known Behavior 135
Known Issues 136
Documentation Updates 138
Migration, Upgrade, and Downgrade Instructions 138
Product Compatibility 141

Documentation Updates

There are no errata or changes in Junos OS Release 19.1R1 documentation for NFX Series.

SEE ALSO

New and Changed Features 132
Changes in Behavior and Syntax 134
Known Behavior 135
Known Issues 136
Resolved Issues 137
Migration, Upgrade, and Downgrade Instructions 138
Product Compatibility 141

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 139](#)
- [Basic Procedure for Upgrading to Release 19.1 | 139](#)

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

Basic Procedure for Upgrading to Release 19.1

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

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

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

To download and install Junos OS Release 19.1R1:

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

SEE ALSO

[New and Changed Features | 132](#)

[Changes in Behavior and Syntax | 134](#)

[Known Behavior | 135](#)

[Known Issues | 136](#)

[Resolved Issues | 137](#)

[Documentation Updates | 138](#)

[Product Compatibility | 141](#)

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 141

Hardware Compatibility

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

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

Hardware Compatibility Tool

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

Software Version Compatibility

This section lists the vSRX and Cloud CPE Solution software releases that are compatible with the Junos OS releases on the NFX Series devices.

NOTE: Starting in Junos OS Release 18.1R1, NFX150 and NFX250 devices support the same version of platform software and vSRX. For example, see [Table 1 on page 141](#).

NFX250 Software Version Compatibility

This section lists the vSRX and CloudCPE Solution software releases that are compatible with the Junos OS releases on the NFX250 devices:

Table 1: Software Compatibility Details with vSRX and Cloud CPE Solution

NFX250 Junos OS Release	vSRX	Cloud CPE Solution
15.1X53-D40.3	15.1X49-D40.6	Cloud CPE Solution 2.0
15.1X53-D41.6	15.1X49-D40.6	Cloud CPE Solution 2.1

Table 1: Software Compatibility Details with vSRX and Cloud CPE Solution (*continued*)

NFX250 Junos OS Release	vSRX	Cloud CPE Solution
15.1X53-D102.2	15.1X49-D61	Cloud CPE Solution 3.0
15.1X53-D47.4	15.1X49-D100.6	Cloud CPE Solution 3.0.1
15.1X53-D490	15.1X49-D143	Cloud CPE Solution 4.0
15.1X53-D495	15.1X49-D160	Cloud CPE Solution 4.1
15.1X53-D496	15.1X49-D170	Cloud CPE Solution 4.1
15.1X53-D45.3	15.1X49-D61	Not applicable
17.2R1	15.1X49-D78.3	Not applicable
17.3R1	15.1X49-D78.3	Not applicable
17.4R1	15.1X49-D78.3	Not applicable
15.1X53-D471	15.1X49-D143	Not applicable
18.1R1	18.1R1	Not applicable
18.1R2	18.1R2	Not applicable
18.1R3	18.1R3	Not applicable
18.2R1	18.2R1	Not applicable
18.3R1	18.3R1	Not applicable
18.3R2	18.3R2	Not applicable
18.4R1	18.4R1	Not applicable

SEE ALSO

[New and Changed Features | 132](#)
[Changes in Behavior and Syntax | 134](#)

[Known Behavior | 135](#)

[Known Issues | 136](#)

[Resolved Issues | 137](#)

[Documentation Updates | 138](#)

[Migration, Upgrade, and Downgrade Instructions | 138](#)

Junos OS Release Notes for PTX Series Packet Transport Routers

IN THIS SECTION

- [New and Changed Features | 144](#)
- [Changes in Behavior and Syntax | 155](#)
- [Known Behavior | 158](#)
- [Known Issues | 159](#)
- [Resolved Issues | 161](#)
- [Documentation Updates | 164](#)
- [Migration, Upgrade, and Downgrade Instructions | 165](#)
- [Product Compatibility | 169](#)

These release notes accompany Junos OS Release 19.1R1 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- [Hardware | 144](#)
- [Authentication, Authorization, and Accounting \(AAA\) | 145](#)
- [Class of Service | 145](#)
- [Forwarding and Sampling | 145](#)
- [Junos Telemetry Interface | 146](#)
- [Layer 3 Features | 148](#)
- [MPLS | 149](#)
- [Multicast | 151](#)
- [Network Management and Monitoring | 151](#)
- [Routing Policy and Firewall Filters | 152](#)
- [Routing Protocols | 152](#)
- [Services Applications | 154](#)

This section describes the new features and enhancements to existing features in Junos OS Release 19.1R1 for the PTX Series.

Hardware

- **QFX10000-60S-6Q line card (PTX10008 and PTX10016 routers)**—Starting with Junos OS Release 19.1R1, the QFX10000-60S-6Q line card provides 60 SFP+ ports that can be configured at either 10-Gbps or 1-Gbps, and six flexible configuration ports for 100-Gbps and 40-Gbps. By default, all the ports will be in the 10-Gbps mode.

Of the six flexible configuration ports, two ports have QSFP28 sockets that support either 100-Gbps, 40-Gbps, or 10-Gbps speeds. The remaining four ports have QSFP+ sockets that can be configured as either a native 40-Gbps port or four 10-Gbps ports using a breakout cable. With breakout cables, the line card supports a maximum of 84 logical 10-GbE ports.

- **Support for 40-Gbps ports to operate at 10-Gbps or 1-Gbps speed (PTX1000, PTX10008, and PTX10016)**—Starting in Junos OS Release 19.1R1, you can use the Mellanox 10-Gbps pluggable adapter (QSFP+ to SFP+ adapter or QSA; model number: MAM1Q00A-QSA) to convert quad-lane based ports to a single-lane based SFP+ port. The QSA adapter has the QSFP+ form factor with a receptacle for the SFP+ module. Use the QSA adapter to convert a 40-gigabit port to a 10-Gbps port or a 1-Gbps port. You can then plug-in a 10-Gbps SFP+ transceiver or a 1-Gbps SFP transceiver into the QSA adapter,

which is inserted into the QSFP or QSFP+ ports of the PTX1000 router or the PTX10K-LC1101 and PTX10K-LC1102 line cards of the PTX10008 and PTX10016 routers.

[See [PTX1000 Transceivers](#), [PTX10008 Transceivers](#) and [PTX10016 Transceivers](#).]

Authentication, Authorization, and Accounting (AAA)

- **Support for SFTP global disablement (PTX Series)**—Starting in Junos OS Release 19.1R1, we have globally disabled incoming SSH File Transfer Protocol (SFTP) connections by default. You can enable incoming SFTP connections globally by configuring the statement **sftp-server** at the **[edit system services ssh]** hierarchy level. Prior to Junos OS Release 19.1R1, the incoming SFTP connections were globally enabled by default.

[See [Configuring sftp-server](#).]

Class of Service

- **Support for class of service (CoS) (PTX10001-20C)**—Starting in Junos OS Release 19.1R1, PTX10001-20C routers support class of service (CoS) functionality for IPv6 traffic. Only default and custom INET, DSPC, and DSPC IPv6 classifiers are supported. Rewrite rules are not supported.

CoS is the assignment of traffic flows to different service levels. Service providers can use router-based CoS features to define service levels that provide different delay, jitter (delay variation), and packet loss characteristics to particular applications served by specific traffic flows.

[See [CoS Features and Limitations on PTX Series Routers](#).]

Forwarding and Sampling

- **Support for tracking static RPM routes across multiple next hops (PTX Series)**—Starting in Junos OS Release 19.1R1, you can use **rpm-tracking** to track up to 16 next hops for RPM-controlled static routes. This features supports both IPv4 and IPv6 static rpm-tracked routes, and extends the single-hop [rpm-tracking](#) introduced in Junos OS Release 18.4.

[See [show route rpm-tracking](#).]

- **Support for using IP addresses in a SR-TE LSP segment list (PTX series)**—Starting in Junos OS Release 19.1R1, you can use IP addresses (IPv4 or IPv6) for next hops in a segment routing traffic engineering (SR-TE) list of label-switched paths (LSPs). This work extends the support for traffic steering based on a segment routing policy that was introduced in Junos OS Release 17.4R1, wherein the controller can specify a segment routing policy consisting of multiple paths to steer labeled or IP traffic.

[See **auto-translate** in [segment-list](#) and **retry-timer** in [source-packet-routing](#) .]

Junos Telemetry Interface

- **Support for the Junos Telemetry Interface (JTI) (PTX10002)**—Starting with Junos OS Release 19.1R1, you can provision sensors through the Junos Telemetry Interface to export telemetry data for several network elements without involving polling. You can stream data through UDP or gRPC.

Only the following sensors are supported on PTX10002 routers:

- Physical interfaces statistics
- Label-switched-path (LSP) statistics
- Network processing unit (NPU) memory
- NPU memory utilization
- CPU memory

To provision sensors to stream data through UDP, all parameters are configured at the **[edit services analytics]** hierarchy level.

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

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

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

- **Transit SPRING sensor support on Junos Telemetry Interface (JTI) (PTX3000 and PTX5000 with FPC2)**—Starting in Junos OS Release 19.1R1, JTI sensor support is available for Source Packet Routing in Networking (SPRING), also known as segment routing. Segment routing is a control-plane architecture that enables an ingress router to steer a packet through a specific set of nodes and links in the network.

Segment routing statistics must first be enabled before the sensor can be configured and statistics streamed to an outside collector by means of JTI.

To enable collection of statistics, configure **set protocols isis source-packet-routing sensor-based-stats per-sid ingress** through the Junos CLI.

To configure the sensor for statistics to be issued to an outside collector, include the following path for either UDP (native) or gRPC streaming:

- **/junos/services/segment-routing/sid/usage/**

For exporting statistics using UDP native sensors, configure parameters at the **[edit services analytics]** hierarchy level.

To provision the sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support the Junos Telemetry Interface (JTI).

[See [sensor \(Junos Telemetry Interface\)](#), [Configuring a Junos Telemetry Interface Sensor \(CLI Procedure\)](#), and [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#).]

- **RSVP interface OpenConfig model support and self-ping logs on Junos Telemetry Interface (JTI) (PTX10003)**—Starting in Junos OS Release 19.1R1, JTI sensor support is enhanced for RSVP interfaces to include delivery of more statistics. The level of support is equivalent to the output delivered when using the **show rsvp interface detail** operational mode command.

To configure the sensor for statistics to be issued to an outside collector, include the following path for gRPC streaming:

- **/network-instances/network-instance/mpls/signaling-protocols/rsvp-te/interface-attributes/interfaces/interface/***

To provision the sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support the Junos Telemetry Interface (JTI).

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

- **Support for LSP statistics on Junos Telemetry Interface (JTI) (PTX10001-20C)**—Starting with Junos OS Release 19.1R1, you can provision the LSP statistics sensor **/junos/services/label-switched-path/usage/** to monitor per-MPLS LSP statistics on the PTX10001-20C router and export telemetry data through JTI to external collectors. You can stream data at configurable intervals through gRPC without involving polling.

JTI support is only for RSVP LSPs.

Statistics that are streamed are similar to the output displayed by the operational mode command **show mpls lsp bypass statistics**.

To provision a sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support the Junos Telemetry Interface (JTI).

To enable statistics for export from the Junos OS, include the **sensor-based-stats** statement at the **[edit protocols mpls]** hierarchy level.

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

- **Export of data associated with the Junos kernel through Junos Telemetry Interface (JTI) (PTX Series)**—Starting in Junos OS Release 19.1R1, you can export data associated with the Junos kernel through remote procedure calls (gRPC) and JTI. Kernel telemetry data includes information on Veriexec state, graceful Routing Engine switchover (GRES), in-service software upgrade (ISSU), and Routing Engine ifstate. Junos kernel sensors can be used by device monitoring and network analytics applications to provide insight into the health status of the Junos kernel.

Junos kernel sensors introduced in Junos OS Release 19.1R1 support both periodical and ON_CHANGE streaming. The following Junos kernel resource paths support periodical streaming only:

- /junos/kernel-ifstate/dead-ifstates-cnt
- /junos/kernel-ifstate/alive-ifstates-cnt
- /junos/kernel-ifstate/delayed-unrefs-cnt
- /junos/kernel-ifstate/delayed-unrefs-max

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

Layer 3 Features

- **Support for Layer 3 unicast features (PTX10001)**—Starting in Junos OS Release 19.1R1, PTX10001 routers support the following Layer 3 forwarding features for unicast IPv4 and IPv6 traffic:
 - Basic IPv6 Forwarding
 - Virtual router (VRF-lite) for both IPv4 and IPv6
 - Layer 3 subinterfaces support for both IPv4 and IPv6
 - VRF-lite, subinterfaces and IPv6 forwarding support on link aggregation group (LAG)
 - Statistics support for Layer 3 subinterfaces
 - 32-way equal-cost multipath (ECMP)
 - Centralized Bidirectional Forwarding Detection (BFD)
 - IPv4 Layer 3 protocols such as
 - OSPF
 - IS-IS
 - BGP
 - IPv6 Layer 3 protocols such as
 - OSPFv3
 - ISISv6

- BGPv6

MPLS

- **Flexible MPLS label stack depth (PTX Series routers with third-generation FPCs)**—Currently, Junos OS supports push of up to a maximum of 5 labels per component of the next hop chain, even though the underlying device capability can be higher. Starting in Junos OS Release 19.1R1, the device capability of pushing more than 5 labels can be leveraged for features, such as, segment routing traffic-engineering (TE) LSPs and RSVP-TE pop-and-forward LSPs.

The number of labels that can be pushed for an MPLS next hop is the number of labels the device is capable of pushing, or the maximum-labels configured under **family mpls** of the outgoing interface, whichever is smaller.

[See [Configuring the Maximum Number of MPLS Labels, maximum-labels](#).]

- **Support for MPLS ping and traceroute for segment routing (PTX Series)**—Starting in Junos OS Release 19.1R1, MPLS ping and traceroute are supported for segment routing (SR) for protocols ISIS and OSPF over IPv4. This feature also supports ECMP traceroute for protocols ISIS and OSPF.

In Junos OS Release 19.1R1, MPLS ping and traceroute for segment routing supports IPv4 IGP-Prefix segment FEC validation. FEC validation for IGP-Adjacency Segment ID is not supported.

[See [ping mpls segment routing isis](#), [ping mpls segment routing ospf](#), [traceroute mpls segment-routing ospf](#), [traceroute mpls segment-routing isis](#).]

- **Enhancements to MPLS for LSP path selection (PTX Series)**—Starting in Junos OS Release 19.1R1, the following enhancements to MPLS have been added for LSP path selection and optimization:

- Earlier when LSP active paths were modified, the LSP path gets cleared and gets resignalled immediately. From Junos OS Release 19.1R1 onwards, if a secondary path is available, then Junos OS selects the secondary path as active, clears and resignals the primary path after the expiry of the **optimize-hold-dead-delay** timer. When the primary LSP path is established, the **revert-timer** gets started. After the **revert-timer** expires, the primary LSP path becomes active.

If the primary LSP path is not active with **revert-timer** on and when there is a change to the primary LSP path, then the LSP path gets cleared and resignalled immediately. When the primary LSP path is established, the revert-timer gets restarted.

- Earlier if there was any Constrained Shortest Path First (CSPF) failure then the current LSP path becomes invalid because it did not match with the configured constraints. In this case, the current LSP path gets cleared immediately. From Junos OS Release 19.1R1 onwards, if a secondary LSP path is available, then Junos OS selects the secondary LSP path as active and clears the primary path after the expiry of the **optimize-hold-dead-delay** timer.

- The CLI knob **no-bypass-statistics-polling** added under the `[edit protocols mpls statistics]` hierarchy now provides information on bypass LSP statistics.
- A new CLI knob **delay** has been introduced under the `[edit protocols mpls optimize-adaptive-teardown]` hierarchy and the value for delay is in the range of (3..65535 seconds). When the **adaptive-teardown** configuration is triggered, the **delay** CLI knob further delays the tearing down of old optimized LSP paths based on the configured value.

[See [statistics \(Protocols MPLS\)](#), [optimize-adaptive-teardown](#).]

- **Use of SID labels as first hop for resolving non-colored static segment routing LSPs (PTX Series)**—Currently, for a static non-colored segment routing traffic-engineered LSP to be usable, the first hop of the segment list must be an IP address. Only the second to *n*th hop could be segment identifier (SID) labels. Starting in Junos OS Release 19.1R1, this requirement does not apply. You can now configure SID labels as the first hop in the segment list.

With this configuration, static non-colored segment routing LSPs are resolved using MPLS fast reroute (FRR) and weighted equal-cost multipath. Without this configuration, by default, the LSPs are resolved using IP address.

[See [Static Segment Routing Label Switched Path](#).]

- **Support of install statement for segment routing LSPs (PTX Series)**—The install *destination-prefix* statement which is currently supported at the `[edit protocols mpls label-switched-path lsp-name]` and `[edit protocols mpls static-label-switched-path lsp-name ingress]` hierarchy levels is now also supported at the `[edit protocols source-packet-routing source-routing-path lsp-name]` hierarchy level for both colored and non-colored static segment routing label-switched paths (LSPs).

You can associate one or more prefixes with a segment routing LSP using the **install** statement. When the LSP is up, all the prefixes are installed as entries into the **inet.3** or **inet6.3** routing table.

[See [install \(Protocols MPLS\)](#).]

- **Control transport address used for targeted-LDP session (PTX Series)**—Currently, only the router-ID or interface address is used as the LDP transport address. Starting in Junos OS Release 19.1R1, you can configure any other IP address as the transport address of targeted LDP sessions, session-groups, and interfaces. This new configuration is applicable only for configured LDP neighbors that have Layer 2 circuit, MPLS, and VPLS adjacencies.

This feature is beneficial when you have multiple loopback interface addresses, and different IGPs associated with LDP interfaces, and you can control the session established between targeted LDP neighbors with the configured transport address.

[See [Control Transport Address Used for Targeted-LDP Session](#).]

- **MPLS egress traffic statistics for label IS-IS routes at ingress device (PTX Series)**—Currently, sensors are available for collecting segment routing statistics for MPLS transit traffic, which is MPLS-to-MPLS in nature. Starting in Junos OS Release 19.1R1, additional sensors are introduced to collect segment routing statistics for MPLS egress traffic at the ingress provider edge (PE) device, which is IP-to-MPLS in nature.

With this feature, you can enable sensors for label IS-IS segment routing egress traffic only, and stream the statistics to a gRPC client.

[See [Understanding Source Packet Routing in Networking \(SPRING\)](#).]

- **Policy-based multipath routes (PTX Series)**—In segment routing networks with multiple protocols in the core, you can combine segment routing traffic-engineered (SR-TE) LDP routes and SR-TE IP routes to create a multipath route that is installed in the routing information base (also known as routing table). You can resolve BGP service routes over the multipath route through policy configuration and steer traffic differently for different prefixes.

[See [Policy-Based Multipath Routes Overview](#).]

Multicast

- **Support for next-generation MVPN Inter-AS option B (PTX)**—Starting in Junos OS Release 19.1R1, for improved security and scalability, Juniper supports Rosen Inter-AS option B for next-generation multicast virtual private networks (MVPNs) and segmented provider tunnels. Only specific configurations are supported, so for example, static tunnels (such as RSVP-TE and IR) are not supported, nor are PIM any-source multicast (ASM) and PIM source-specific multicast (SSM) tunnels.

In the supported configuration, next-generation MVPN sites can span multiple autonomous system (AS) boundaries (that is, domains). Each AS can implement its own p-tunnel (they don't have to be the same). Per-VPN subinterfaces are not shared between ASBRs. Likewise, provider edge (PE) routers from one AS cannot be reached from another AS, and the AS topology of one site is not exposed to any others.

[See [inter-as \(Routing Instances\)](#) and [BGP-MVPN Inter-AS Option B Overview](#).]

Network Management and Monitoring

- **sFlow performance improvements (PTX Series)**—Starting in Junos OS Release 19.1R1, the following improvements have been added to the sFlow technology feature:
 - For MX Series, PTX Series, and QFX Series, you can configure forwarding class and DSCP values per collector.
 - For PTX Series and QFX Series, you can configure IPv6 addresses for the **source-ip** and **agent-id**.
 - Enhancements are made to the following CLI commands: **show sflow collector**, **show sflow collector address ip-address**, and **show sflow interface**.

[See [Understanding How to Use sFlow Technology for Network Monitoring](#), [collector](#), [agent-id](#), [source-ip](#), [show flow collector](#), and [show flow interface](#).]

Routing Policy and Firewall Filters

- **Support for IPv6 firewall filters (PTX100020C)**— Starting with Junos OS Release 19.1R1, you can configure a firewall filter with match conditions for IPv6 traffic (ingress direction only). You configure firewall filters under the **[edit firewall]** hierarchy level.

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

[See [IPv6 Firewall Filter Match Conditions and Actions \(PTX10001-20C\)](#).]

Routing Protocols

- **Support for BGP graceful shutdown (PTX Series)**— Starting in Junos OS Release 19.1R1, graceful traffic migration from one BGP next hop to another is supported, without traffic interruption. Also, BGP administrative shutdown communication can be sent to the BGP peer.

You can configure both **graceful-shutdown** and **shutdown** statements at the **[edit protocols bgp]**, **[edit protocols bgp group group-name]**, and **[edit protocols bgp group group-name neighbor address]** hierarchy levels.

NOTE: Graceful shutdown is disabled by default.

[See: [graceful-shutdown \(Protocols BGP\)](#), [shutdown \(Protocols BGP\)](#).]

- **Support for configurable SRGB used by SPRING in OSPF protocols (PTX Series)**— Starting in Junos OS Release 19.1R1, you can configure the segment routing global block (SRGB) range label used by segment routing. Labels from this range are used for segment routing functionality in OSPF domain.

The SRGB is a range of the label values used in the segment routing. Prior to Junos OS Release 19.1R1, you could not configure the range for the SRGB block.

Locally you can configure **srgb start-label <label-range> index-range <index-range>** command under **[edit protocols ospf source-packet-routing]** hierarchy or globally under **[edit protocols mpls label-range]** hierarchy.

Following are the SRGB precedences for OSPF protocol:

- Local SRGB
- Global SRGB
- Node-segment implementation of 256 label block

[See [source-packet-routing \(Protocols IS-IS and OSPF\)](#).]

- **Support for BGP advertising aggregate bandwidth across external BGP links for load balancing (PTX Series)**—Starting in Junos OS Release 19.1R1, BGP uses a new link bandwidth extended community, **aggregate-bandwidth**, to advertise an aggregated bandwidth of multipath routes across external links. BGP calculates the aggregate of multipaths that have unequal bandwidth allocation and advertises the aggregated bandwidth to external BGP peers. A threshold to the aggregate bandwidth can be configured to restrict the bandwidth usage of a BGP group. In earlier Junos OS releases, a BGP speaker receiving multipaths from its internal peers advertised the link bandwidth associated with the active route.

To advertise the aggregated bandwidth of multipath routes and to set a maximum threshold, configure a policy with the **aggregate-bandwidth** and **limit bandwidth** actions at the **[edit policy-options policy-statement *name* then]** hierarchy level.

[See [Advertising Aggregate Bandwidth Across External BGP Links for Load Balancing Overview](#).]

- **Support for policy-based allocation for IPv4 BGP-labeled unicast (PTX Series)**—Starting in Junos OS Release 19.1R1, this feature supports:
 - Allocating policy-based labels for IPv4 BGP-LU prefixes in per-prefix label allocation mode
 - 1:1 mapping between prefixes and labels
 - Map policy for labels
 - Fallback actions of dynamic and reject for handling error conditions

[See [policy-options](#), [route-filter-list](#).]

- **Support for BGP link-state distribution with SPRING extensions (PTX Series)**—Starting in Junos OS Release 19.1R1, BGP link-state extensions export segment routing topology information to software-defined networking controllers. Controllers can get the topology information by either being a part of an interior gateway protocol (IGP) domain or through BGP link-state distribution.

BGP link-state distribution is supported on inter-domain networks and provides a scalable mechanism to export the topology information. This feature benefits networks that are moving to source packet routing in networking (SPRING) but also have RSVP deployed, and continue to use both SPRING and RSVP in their networks.

In this release, OSPF link-state protocol is supported which pushes SPRING information to the BGP link-state address family.

[See [Link-State Distribution Using BGP Overview](#).]

- **Scalability for LDP-over-RSVP and BGP labelled unicast services (PTX Series)**—Starting in Junos OS Release 19.1R1, this feature enhances RPD to produce the chain nexthop for various services. The RPD is enhanced to do build a translation layer between RIB and FIB to segment multi-protocol transport tunnels.

Segmentation happens as follows:

- Only LDP, RSVP, LDP-over-RSVP, LDP-over-RSVP-over-BYPASS ingress tunnels are considered for segmentation.
- Segmentation does not happen if there is only one label in the stack.
- Segmentation happens at the app boundary. A nexthop with two LDP labels in its stack or two RSVP labels will not be split into two nexthops with one label each.

Any route resolution over LDP or LDP-over-RSVP is changed from INH->FNH to CNH->INH->CNH->FNH in kernel and PFE and for LDP routes in INET.3. Where indirect nexthop (INH) is an application installed in direction towards the final nexthop (FNH). Any segmented stack introduces the composite chain nexthop (CNH) where the segmented portion of the label stack precedes an INH, or an FNH. The chain is collapsed and the resulting label stack is encoded in the packet header by the hardware before forwarding the packet.

By chaining labels instead of stacking them, PTX memory is made available for FNH label operations, as well as CNH by grouping CNHs within the same unilist nexthop (for ECMP) based on the label space identifier.

The following applications are supported:

- Transit
 - LBGP stitching with LDP over RSVP
- Ingress
 - 6PE BGP-V6-Route->LBGP(Explicit V6 NULL label) over LDP over RSVP
 - 4PE BGP-V4-Route->LBGP(Explicit V4 NULL label) over LDP over RSVP
 - BGP-L3VPN over LDP over RSVP
 - BGP-V6-VPN over LDP over RSVP
- BGP route with indirection resolving over LDP over RSVP
 - IBGP-V4-ROUTE over LDP over RSVP
 - IBGP-V6-ROUTE over LDP over RSVP

[See [Tunneling LDP LSPs in RSVP LSPs Overview](#), [BGP Route Resolution Overview](#).]

Services Applications

- **Support for IPv4 and IPv6 inline active flow monitoring on IRB interfaces (PTX1000)**—Starting in Junos OS Release 19.1R1, you can perform inline active flow monitoring for IPv4 and IPv6 traffic on integrated routing and bridging (IRB) interfaces. Both IPFIX and version 9 templates are supported.

IRB interfaces enable a switch to identify packets that are being sent to local addresses to be bridged whenever possible and to be routed only when required. Switching or bridging uses fewer layers of processing than routing, thus reducing the number of address lookups.

[See [Inline Active Flow Monitoring on IRB interfaces.](#)]

- **Support for automatic restart of Two-Way Active Measurement Protocol (TWAMP) Client (PTX Series)**—Starting in Junos OS Release 19.1R1, the TWAMP client restarts automatically after a network failure, a configuration change, or an IP connectivity issue. However, for the client to reconnect to the TWAMP server automatically, you must use 0 as the *test-count* value in the **set rpm twamp client control-connection test-count** command. Also, at the TWAMP server side, the default value of *max-connection-duration* in the **set rpm twamp server max-connection-duration** must also be 0. You can display the test results after the network recovers, or after the server is reachable, by using the **set services rpm twamp client control-connection c1 persistent-results** command.

[See [Understanding TWAMP Auto-Restart.](#)]

- **Port mirroring support for the IPv6 address family (PTX10001)**—Starting in release 19.1R1, Junos OS supports port mirroring on the PTX10001 router for the IPv6 address family. Port mirroring copies packets entering or exiting a port 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. The PTX Series supports the IPv6 (inet6) address family only.

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

SEE ALSO

Changes in Behavior and Syntax	 155
Known Behavior	 158
Known Issues	 159
Resolved Issues	 161
Documentation Updates	 164
Migration, Upgrade, and Downgrade Instructions	 165
Product Compatibility	 169

Changes in Behavior and Syntax

IN THIS SECTION

- [Interfaces and Chassis](#) | [156](#)
- [Network Management and Monitoring](#) | [156](#)

- Services Applications | 157
- User Interface and Configuration | 157

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 19.1R1 for the PTX Series.

Interfaces and Chassis

- **New XML tag element <lacp-hold-up-state> added in show lacp interfaces XML display (PTX Series)**—Starting in Junos OS Release 19.1R1, the **show lacp interfaces | display xml** command displays a new XML tag element **<lacp-hold-up-state>**. The **<lacp-hold-up-state>** displays the time interval an interface holds before it changes from state, down to up. In earlier Junos OS releases, the LACP hold-up information for all interfaces was in a single **<lacp-hold-up-information>** XML tag. Now, for each interface it is displayed in a separate **<lacp-hold-up-information>** XML tag.
- **Support for creating layer 2 logical interface independently (PTX Series)**—Starting in Junos OS Releases 18.4R1, 18.4R2, 19.1R1, 19.1R2, and later, PTX Series routers support creating layer 2 logical interface independent of layer 2 routing instance type. That is, you can configure and commit the layer 2 logical interfaces separately and add the interface to bridge-domain or Ethernet VPN (EVPN) routing instance separately. Note that the layer 2 logical interfaces works fine only when the interface is added to bridge domain or EVPN routing instance.

In the earlier Junos OS releases, when a layer 2 logical interface configuration (units with encapsulation vlan-bridge configuration) is used, then the logical interface must be added as part of a bridge-domain or EVPN routing instance for the commit to succeed.

Network Management and Monitoring

- **Change in error severity (PTX10016)**—Starting in Junos OS Release 19.1R1, on PTX10016 routers, the severity of the FPC error, shown in the syslog as **PE Chip::FATAL ERROR!! from PE2[2]: RT: Clear Fatal if it is detected LLMEM Error MEM:llmem, MEMTYPE: 1**, is changed from fatal to non-fatal (or minor). In case of this error, only a message is displayed for information purposes. To view the error details, you can use the show commands **show chassis fpc errors** and **show chassis errors active**.
[See [show chassis fpc errors](#).]
- **NETCONF <kill-session> operation returns different values in <rpc-error> when the session identifier is equal to the current session ID (PTX Series)**—Starting in Junos OS Release 19.1R1, when you execute the **<kill-session>** NETCONF operation and the session identifier is equal to the current session ID, the values of the **<error-type>** and **<error-tag>** elements in the resulting **<rpc-error>** are **application** and

invalid-value, respectively. In earlier releases, the **<error-type>** and **<error-tag>** values are **protocol** and **operation-failed**.

[See [<kill-session>](#).]

Services Applications

- **Support for enabling hardware timestamping of RPM probe messages (PTX Series)**—Starting in Junos OS Releases 19.1R1, PTX Series routers support timestamping of RPM probe messages on the Packet Forwarding Engine. The following configuration statements at the **[edit services rpm probe owner test test-name]** hierarchy level are supported:
 - **hardware-timestamp**—To enable timestamping of RPM probe messages in the Packet Forwarding Engine host processor.
 - **one-way-hardware-timestamp**—To enable timestamping of RPM probe messages for one-way delay and jitter measurements.

These features are supported only with icmp-ping, icmp-ping-timestamp, udp-ping, and udp-ping-timestamp probe types.

User Interface and Configuration

- **Options for monitor traffic interfaces statement added (PTX Series)**—Starting in Junos OS Release 19.1R1, the options **write-file** and **read-file** under the **monitor traffic** command are included in the visible CLI.
- [See [monitor traffic](#).]

SEE ALSO

New and Changed Features 144
Known Behavior 158
Known Issues 159
Resolved Issues 161
Documentation Updates 164
Migration, Upgrade, and Downgrade Instructions 165
Product Compatibility 169

Known Behavior

IN THIS SECTION

- [General Routing | 158](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 19.1R1 for the PTX Series.

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

General Routing

- When an FPC goes offline or restarts, FPC x sends traffic to FPC y. The following error messages are seen and a corresponding alarm is set on the destination FPC. Specific to PTX10000, the transient alarm gets set when this condition occurs. The alarm clears later because the source FPC goes offline. **Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Error (0x210613), module: PE Chip, type: Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Cmerror Op Set: PE Chip: PE1[1]: FO:core intr: 0x00000010: Grant spray drop due to unspray-able condition error Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Error (0x210614), module: PE Chip, type: Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Cmerror Op Set: PE Chip: PE1[1]: FO:core intr: 0x00000008: Request spray drop due to unspray-able condition error.** [PR1268678](#)
- On PTX1000 and MX Series, sFlow technology sampling output has different VLAN priority in extended switch data fields with the same dual-tag configuration when **egress sampling** is configured. This is dependent on the sequence in which sampling and mac-rewrite happens. On MX Series, MAC rewrite occurs after sampling and PTX Series, sampling happens after MAC rewrite. [PR1387468](#)
- Frames cannot be fragmented and are larger than the outgoing interface MTU size will be dropped; however, the **show interface statistics extensive** output might not show these dropped frames against output errors and MTU errors. [PR1408576](#)
- In case of stacked VLAN tagging, VLAN tagged frame counters are not supported for LC1101, LC1102, and LC1103 Series card in PTX Series routers. [PR1412987](#)

SEE ALSO

[New and Changed Features | 144](#)

Changes in Behavior and Syntax	155
Known Issues	159
Resolved Issues	161
Documentation Updates	164
Migration, Upgrade, and Downgrade Instructions	165
Product Compatibility	169

Known Issues

IN THIS SECTION

- General Routing | 159
- Interfaces and Chassis | 161
- Routing Protocols | 161

This section lists the known issues in hardware and software in Junos OS Release 19.1R1 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

- On the third-generation PTX Series routers FPCs (PTX3000, PTX5000 FPC3, and PTX1000) if the **protocols mpls no-propagate-ttl** command is configured, the MPLS TTL field can be reset to 255 in the packets where a label swap operation is performed. [PR1287473](#)
- On a PTX Series PIC with the CFP2-DCO-T-WDM transceiver installed, after repeated configuration rollbacks, the link sometimes takes a long time to come up. [PR1301462](#)
- When CFP2-DCO-T-WDM-1 plugged in PTX Series PIC, after FPC restart sometimes carrier frequency offset TCA is raised even when TCA is not enabled. [PR1301471](#)
- In the specific case of semigraceful RCB reboot initiated by the internal shell command **vhclient init 0**, GRES takes longer to complete; that is, 3 minutes as opposed to 21 seconds. The regular CLI command **request vmhost reboot** (graceful) and a jack-out-jack-in of the Routing Engine (ungraceful) do not exhibit this delay. [PR1312065](#)

- On a PTX Series router with a third-generation FPC, an error message is displayed when the FPC goes online or offline. [PR1322491](#)
- This issue occurs on 30-port MACsec linecard (LC1101-M - 30C / 30Q / 96X) of PTX10000 chassis, under certain circumstances, with an **exclude-protocol lacp** configuration under the **[edit security macsec connectivity-association connectivity-association-name]** hierarchy level is deleted or deactivated. The LACP "Mux State" shown under the output of the CLI command **show lacp interface** might remain as "attached" or "detached" and might not transit to "distributing" state. [PR1331412](#)
- The output of the CLI command **show class-of-service fabric statistics** now includes traffic that was dropped because of internal errors in the drop counts. [PR1338647](#)
- The Routing Engine boots from the secondary disk when you:
 - Press the reset button, on the RCB front panel, while the Routing Engine is booting up but before Junos OS is up
 - Upgrade software by booting from the network using the **request vmhost reboot** network command, and the system fails to boot from the network
 - Upgrade BIOS and the upgrade fails
 - Reboot and the system hangs before Junos OS is up [PR1344342](#)
- User might not be able to stop the ZTP bootstrap when a PTX10016 and PTX10008 router with a certain number of line cards is powered on with the factory-default configuration. [PR1369959](#)
- When a Routing Engine reboots and comes up again, it sends gratuitous ARP packets to the internal interfaces in order to advertise its MAC address. These packets get to the UKERN running on the FPC, which drops these packets. Error messages are printed just before dropping these packets. These error messages are harmless and do not disrupt the functioning of any feature. [PR1374372](#)
- Control plane switch management (CPSM) daemon memory leak occur in VMHOST. As a result, log rotate might not work, causing large cpsm log size. [PR1387903](#)
- In Dynamic Host Configuration Protocol (DHCPv6) relay scenario, the DHCPv6 relay-reply packet might be dropped by the DHCP relay when sent back to the client. The issue results in DHCPv6 client binding failure. [PR1399683](#)
- On PTX3000 platform with several FPCs (for example, around 8), after reloading the chassis, FPCs might not be able to come online for twenty minutes or longer. [PR1404611](#)
- On PTX10008 and PTX10016 routers the image upgrade using ZTP fails when you have more than one WAN interfaces from PTX10,000 router to the DHCP server. [PR1404832](#)
- On PTX Series routers, a auto correctable non-fatal hardware error on PE chip (which is ASIC on PTX1000 and PTX10002, the third-generation FPC on PTX3000 or PTX5000, and the line card on PTX10008 or PTX10016) is reported as 'FATAL' error. Therefore, the relevant Packet Forwarding Engine will get disabled. The code changes have been made to change the error category from 'FATAL' to 'INFO' to avoid the Packet Forwarding Engine to be disabled unexpectedly. [PR1408012](#)

- Sequence number does not get reset after changing reporting interval for the physical interface sensor. [PR1410651](#)
- Sometimes the SFP+ read does not work on one or more ports of the "LC1103-2C/6Q/60X". If this happens, the corresponding SFP+ module will not get detected and will not be displayed at the Routing Engine CLI under the output of **show chassis hardware**. As a workaround, reseal the SFP+ module. [PR1412897](#)

Interfaces and Chassis

- Upgrading Junos OS Release 14.2R5 and later maintenance releases and Junos OS Release 16.1 and later mainline releases with CFM configuration might cause the cfmd process to crash after upgrade. This is because of the old version of **/var/db/cfm.db**. [PR1281073](#)

Routing Protocols

- In segment routing scenario, syslog message is seen whenever prefix-sid coincides with the node-sid. These logs are causing confusion and incorrectly reports duplicate node segment ID duplication. There is no service impact. [PR1403729](#)

SEE ALSO

[New and Changed Features | 144](#)

[Changes in Behavior and Syntax | 155](#)

[Known Behavior | 158](#)

[Resolved Issues | 161](#)

[Documentation Updates | 164](#)

[Migration, Upgrade, and Downgrade Instructions | 165](#)

[Product Compatibility | 169](#)

Resolved Issues

IN THIS SECTION

• [General Routing | 162](#)

• [Interfaces and Chassis | 163](#)

- MPLS | 163
- Platform and Infrastructure | 163
- Routing Protocols | 164

This section lists the issues fixed in Junos OS Release 19.1R1 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

- Repeated log messages `%PFE-3 fpcX expr_nh_index_tree_ifl_get` and `expr_nh_index_tree_ipaddr_get` are observed when sampling packet is discarded with log (or syslog) statement under firewall filter. [PR1304022](#)
- On PTX Series platform, multicast traffic packet drop seen is more than 50 percent when having FPC1/FPC2 mix with FPC3. [PR1339481](#)
- On PTX10001 platform, the FRR link-protection convergence during FRR and MBB with various MPLS optimize-timers is observed. [PR1355953](#)
- The netproxy service client component fails to start after issuing **request vmhost reboot** command. [PR1365664](#)
- The IPLC card might take a long time to come up after requesting it online from an offline state. [PR1368637](#)
- Some harmless log messages are suppressed on the backup SPMB. [PR1369731](#)
- On PTX10001 platform, 100G-LR4 optics and 100G-ER4 optics are not supported. [PR1371590](#)
- Inline BFD might keep flapping when inline sampling is configured. [PR1376509](#)
- Traffic might be dropped on third-generation FPCs on PTX Series routers. [PR1378392](#)
- BFD sessions flap when restarting one FPC on PTX10000. [PR1383703](#)
- Packet Forwarding Engine based local repair does not happen for IP routes pointing to unilist of composites with indirect next hops. [PR1383965](#)
- Disable reporting of correctable single-bit error on Hybrid Memory Cube (HMC) and prevent the major alarm. [PR1384435](#)
- Packet drop might be seen in AF3 queue on PTX Series platforms. [PR1385454](#)
- The system might hang after issuing **request system reboot**. [PR1386279](#)

- BFD flaps are seen on PTX Series platforms with inline BFD. [PR1389569](#)
- Forwarding issue on mixed link-speed aggregated Ethernet interface after FPC reloads. [PR1390417](#)
- PTX10002-60C FPC might not be detected after the ukern crashes. [PR1396507](#)
- High jsd or na-grpcd CPU usage might be seen even when JET or JTI is not used. [PR1398398](#)
- CPU hog might be observed on PTX Series platform. [PR1399369](#)
- Log message **JAM HW data base open failed for ptx5kpic_3x400ge-cfp8** occurs during commit. [PR1403071](#)
- On PTX3000 FPCs are not able to come online for tens of minutes after a reboot of the chassis. [PR1404611](#)
- 100G SR4 optics with part number 740-061405 should be displayed as **QSFP-100G-SR4-T2**. [PR1405399](#)
- Layer 2 VPN flaps repeatedly after link up between PE and CE devices under "asynchronous-notification" and "some types of MICs" conditions. [PR1407345](#)
- For PTX10001-20C devices, the DHCP relay functionality and binding of DHCP does not work. [PR1407476](#)
- On PTX3000 router, the rpd crash is observed at `if_addr_link`, `krt_chnh_template_create_restart`, `krt_chnh_create_restart`, `krt_comp_add_comp_nh`, `krt_build_comp_nh`, `krt_build_nexthop`, `krt_rt_add_sock`, `krt_decode_rt`, `krt_sysctl_read_consume`, `krt_rt_read`, `krt_sys_rtread`, `krt_var_init`, `ctx_handle_node`, `ctx_walk_features`, `task_read_config`, `main`. [PR1409051](#)

Interfaces and Chassis

- PE Chip:pe0[0]: IPW: **oversize_drop error** causes major error on FPC. [PR1375030](#)

MPLS

- MPLS LSP will remain in down state because of routing loop detection after flapping link between PE router and egress PE. [PR1384929](#)
- The rpd might crash when LDP route with indirect next hop is deleted. [PR1398876](#)
- A single-hop bypass LSP might not be used for traffic when both transit chaining mode and sensor-based-stats are used. [PR1401152](#)

Platform and Infrastructure

- On PTX Series routers, the **RPM hardware-timestamp** and **one-way-hardware-timestamp** statements are not enabled. [PR1399842](#)
- When non-root user tries to archive the **var/log** some files are missing from the cscript.log file. [PR1405903](#)

Routing Protocols

- The rpd process generates a core file on the backup Routing Engine during neighborship flap when using authentication-key with size larger than 20 characters. [PR1394082](#)
- The rpd RT_NEXTHOPS_TEMPLATE memory leaks while using segment routing for IS-IS protocols. [PR1404134](#)

SEE ALSO

New and Changed Features 144
Changes in Behavior and Syntax 155
Known Behavior 158
Known Issues 159
Documentation Updates 164
Migration, Upgrade, and Downgrade Instructions 165
Product Compatibility 169

Documentation Updates

There are no errata or changes in Junos OS Release 19.1R1 documentation for the PTX Series.

SEE ALSO

New and Changed Features 144
Changes in Behavior and Syntax 155
Known Behavior 158
Known Issues 159
Resolved Issues 161
Migration, Upgrade, and Downgrade Instructions 165
Product Compatibility 169

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading to Release 19.1 | 165](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 168](#)
- [Upgrading a Router with Redundant Routing Engines | 168](#)

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.

Basic Procedure for Upgrading to Release 19.1

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

NOTE: Back up the file system and the currently active Junos OS configuration before upgrading Junos OS. This allows you to recover to a known, stable environment if the upgrade is unsuccessful. Issue the following command:

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

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

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

To download and install Junos OS Release 19.1R1:

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

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

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

```
user@host> request system software add validate reboot  
source/junos-install-ptx-x86-64-19.1R1.9.tgz
```


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

```
user@host> request system software add validate reboot  
source/junos-install-ptx-x86-64-19.1R1.9-limited.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

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

NOTE: After you install a Junos OS Release 19.1**jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.4, 18.1, and 18.2 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

Upgrading a Router with Redundant Routing Engines

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

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

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

SEE ALSO

[New and Changed Features | 144](#)

[Changes in Behavior and Syntax | 155](#)

[Known Behavior | 158](#)

[Known Issues | 159](#)

[Resolved Issues | 161](#)

[Documentation Updates | 164](#)

[Product Compatibility | 169](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 169](#)

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 explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://apps.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 | 144](#)

[Changes in Behavior and Syntax | 155](#)

[Known Behavior | 158](#)

[Known Issues | 159](#)

[Resolved Issues | 161](#)

[Documentation Updates | 164](#)

[Migration, Upgrade, and Downgrade Instructions | 165](#)

Junos OS Release Notes for the QFX Series

IN THIS SECTION

- New and Changed Features | 170
- Changes in Behavior and Syntax | 184
- Known Behavior | 187
- Known Issues | 189
- Resolved Issues | 195
- Documentation Updates | 200
- Migration, Upgrade, and Downgrade Instructions | 201
- Product Compatibility | 215

These release notes accompany Junos OS Release 19.1R1 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

- Hardware | 172
- Authentication, Authorization and Accounting (AAA) (RADIUS) | 172
- Class of Service (CoS) | 172
- EVPNs | 173
- Forwarding and Sampling | 173
- General Routing | 174
- Interfaces and Chassis | 177
- Junos Telemetry Interface | 178
- Layer 2 Features | 179

- Licensing | 179
- Management | 180
- MPLS | 180
- Network Management and Monitoring | 181
- Routing Policy and Firewall Filters | 182
- Routing Protocols | 182
- System Management | 184

This section describes the new features and enhancements to existing features in Junos OS Release 19.1R1 for the QFX Series.

NOTE: The following QFX Series platforms are supported in Release 19.1R1: QFX5100, QFX5110 (32Q & 48S), QFX5120, QFX5200, QFX5210, QFX10002, QFX10002-60C, QFX10008, and QFX10016.

Hardware

- **QFX5120-32C switches**— Starting with Release 19.1R1, Junos OS supports the fixed-configuration QFX5120-32C switch. This switch provides 100-Gbps spine-and-leaf connectivity in Layer 2 and Layer 3 fabrics for cloud and Web services.

The QFX5120-32C has 2 SFP+ ports that operate at 10-Gbps speed, and 32 ports that can operate at 40-Gbps (with QSFP+ transceivers) and 100-Gbps speeds (with QSFP28 transceivers). You can use breakout cables to channelize the 40-Gbps ports into four 10-Gigabit Ethernet interfaces and the 100-Gbps ports into four 25-Gigabit Ethernet interfaces.

The QFX5120-32C is available with AC power supplies and with front-to-back or back-to-front airflow.

Authentication, Authorization and Accounting (AAA) (RADIUS)

- **Support for SFTP global disablement (QFX Series)**—Starting in Junos OS Release 19.1R1, we have globally disabled incoming SSH File Transfer Protocol (SFTP) connections by default. You can enable incoming SFTP connections globally by configuring the statement **sftp-server** at the **[edit system services ssh]** hierarchy level. Prior to Junos OS Release 19.1R1, the incoming SFTP connections were globally enabled by default.

[See [Configuring sftp-server](#)]

Class of Service (CoS)

- **Support for per-port buffer monitoring (QFX5000 switches)**—Starting with Junos OS Release 19.1R1, to keep track of peak buffer occupancy for each queue or priority group on a port, you can enable per-port buffer monitoring on a QFX5000 Series switch by setting **buffer-monitor-enable** at the **[edit chassis fpc slot-number traffic-manager]** hierarchy level. You can then monitor the buffer occupancy on the designated ports by executing the **show interfaces priority-group interface-name buffer-occupancy** or **show interfaces queue interface-name buffer-occupancy** command.

[See [traffic-manager](#).]

- **Support for class of service (CoS) on QFX5120-32C switches (QFX Series)**—Starting in Junos OS Release 19.1R1, QFX5120-32C switches support most class of service (CoS) features. IP precedence classification is not supported; DSCP classifiers are supported but can't be set at ingress. Also, as with other QFX5200 series switches, CoS flexible hierarchical scheduling (ETS) is not supported.

CoS is the assignment of traffic flows to different service levels. Service providers can use router-based CoS features to define service levels that provide different delay, jitter (delay variation), and packet loss characteristics to particular applications served by specific traffic flows.

[See [CoS Operational Comparison Between QFX5100, QFX5120, QFX5200, and QFX5210 Switches](#).]

EVPNs

- **EVPN proxy ARP and ARP suppression, and proxy NDP and NDP suppression without IRB interfaces (QFX10000 switches)**—Starting in Junos OS Release 19.1R1, QFX10000 switches that function as Layer 2 VXLAN gateways in an EVPN-VXLAN environment support proxy ARP and ARP suppression, and proxy NDP and NDP suppression on non-IRB interfaces. Now, any interface configured on these Layer 2 VXLAN gateways can deliver ARP and NDP requests from both local and remote devices.

In addition, you can now control the following aspects of the MAC-IP address bindings database on a QFX10000 switch:

- The maximum number of MAC-IP address entries in the database
- The amount of time a locally learned MAC-IP address binding remains in the database

[See [EVPN Proxy ARP and ARP Suppression, and Proxy NDP and NDP Suppression](#).]

Forwarding and Sampling

- **Customizing hashing parameters and shared-buffer alpha values for better load balancing (QFX5100, QFX5110, QFX5200, and QFX5210 switches)**—These switches achieve load balancing through use of a hashing algorithm, which determines how to forward traffic over LAG bundles or to next-hop devices when ECMP is enabled. The hashing algorithm makes hashing decisions based on values in various packet fields. Starting with Junos OS Release 19.1R1, you can explicitly configure some hashing parameters to make hashing more efficient. The shared-buffer pool is a global memory space that all ports on the switch share dynamically as they need buffers. The switch uses the shared-buffer pool to absorb traffic bursts after the dedicated-buffer pool is exhausted. The shared-buffer pool threshold is dynamically calculated based on a factor called “alpha”. Also starting with Junos OS Release 19.1R1, you can specify the alpha, or dynamic threshold, value to determine the change threshold of shared buffer pools for both ingress and egress buffer partitions.

To specify hashing parameters:

```
user@switch# set forwarding-options enhanced-hash-key hash-parameters (ecmp | lag)
```

To specify a threshold value for a particular queue:

```
user@switch# set class-of-service shared-buffer (ingress|egress) buffer-partition buffer
dynamic-threshold value
```

[See [hash-parameters](#) and [buffer-partition](#).]

General Routing

- **Supported features on new hardware (QFX5120-32C)**—Starting with Junos OS Release 19.1R1, the following Junos OS features are supported on QFX5120-32C switches:

- **Layer 2 unicast features:**

- 802.1Q VLAN trunking
- 802.1p
- PVLAN
- Routed VLAN interface (RVI)
- Layer 3 VLAN-tagged logical interfaces
- 4096 VLANs
- MAC address filtering
- MAC address aging configuration
- Static MAC address assignment for interface
- Per-VLAN MAC learning (limit)
- MAC learning disable
- Persistent MAC (sticky MAC)
- Q-in-Q Tag manipulation
- MAC address limit per port
- MAC limiting
- MAC limiting per port, per VLAN
- MAC move limiting
- PVLAN on Q-in-Q
- 802.1D
- 802.1w (RSTP)
- 802.1s (MST)
- BPDU protection
- Loop protection
- Root protection
- VSTP
- RSTP and VSTP running concurrently
- Link aggregation (static and dynamic) with LACP (fast and slow LACP)

- LLDP
- Multiple VLAN Registration Protocol (802.1ak)

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

- **Layer 2 multicast features:**

- IGMP snooping for IGMPv1, IGMPv2, and IGMPv3
- IGMP proxy
- IGMP querier
- Virtual router (VRF-lite) IGMP snooping

[See [Multicast Overview](#).]

- **Layer 3 unicast features:**

- Static routing, ping, and traceroute (IPv4, IPv6)
- OSPFv2 (IPv4) and OSPFv3 (IPv6)
- RIPv2
- BGP (IPv4, IPv6), BGP 4-byte ASN support, and BGP multipath
- MBGP (IPv4)
- IS-IS (IPv4, IPv6)
- BFD (for RIP, OSPF, IS-IS, BGP, PIM)
- Filter-based forwarding (FBF)
- Unicast reverse path forwarding (RPF)
- IP directed broadcast traffic forwarding
- VRRP
- VRRPv3 (IPv6)
- Neighbor Discovery Protocol (IPv6)
- Path MTU discovery
- IPv6 CoS—Behavior aggregate (BA) classifiers, multifield (MF) classifiers and rewrite rules, traffic-class scheduling
- IPv6 stateless address autoconfiguration
- ECMP—32-way
- Hierarchical ECMP
- Virtual router (VRF-lite) IS-IS, RIP, OSPF, BGP

[See [BGP User Guide](#), [IPv6 Neighbor Discovery User Guide](#), [IS-IS User Guide](#), [OSPF User Guide](#), [Protocol-Independent Routing Properties User Guide](#), and [RIP User Guide](#).]

- **Layer 3 multicast features:**

- IGMP version 1 (IGMPv1), version 2 (IGMPv2), and version 3 (IGMPv3)
- IGMP filtering
- PIM sparse mode (PIM-SM)
- PIM source-specific multicast (PIM-SSM)
- PIM dense mode (PIM-DM)
- Virtual router (VRF-lite) PIM, IGMP
- Multicast Source Discovery Protocol (MSDP)

[See [Multicast Overview](#).]

- **VXLAN features:**

- EVPN-VXLAN—Layer 2 and Layer 3 VXLAN gateways
 - Pure type-5 routes. [See [EVPN Type-5 Route with VXLAN encapsulation for EVPN-VXLAN](#).]
 - IGMP snooping. [See [Overview of IGMP Snooping in an EVPN-VXLAN Environment](#).]
 - Tunneling of Q-in-Q traffic. [See [Examples: Tunneling Q-in-Q Traffic in an EVPN-VXLAN Overlay Network](#).]
 - Support for OSPF, IS-IS, BGP, and static routing on IRB interfaces. [See [Supported Protocols on an IRB Interface in EVPN-VXLAN](#).]
 - Support for IPv6 data traffic. [See [Routing IPv6 Data Traffic through an EVPN-VXLAN Network with an IPv4 Underlay](#).]
 - MAC mobility. [See [Overview of MAC Mobility](#).]
 - EVPN proxy ARP and ARP suppression, and NDP and NDP suppression. [See [EVPN Proxy ARP and ARP Suppression, and NDP and NDP Suppression](#).]
- OVSDB-VXLAN—Layer 2 VXLAN gateway. [See [Understanding the OVSDB Protocol Running on Juniper Networks Devices](#).]
- PIM-based Layer 2 VXLAN gateway. [See [Examples: Manually Configuring VXLANs on QFX Series and EX4600 Switches](#).]
- MPLS support. [See [MPLS Feature Support on QFX Series and EX4600 Switches](#).]
- Multichassis link aggregation group (MC-LAG). [See [Multichassis Link Aggregation Features, Terms, and Best Practices](#).]
- **Services support:**
 - sFlow. [See [Overview of sFlow Technology](#).]

- Port mirroring. [See [Understanding Port Mirroring](#).]
- Storm control. [See [Understanding Storm Control](#).]
- Resilient hashing support for LAGs and ECMP routes. [See [Understanding the Use of Resilient Hashing to Minimize Flow Remapping in Trunk/ECMP Groups](#).]
- Distributed denial of service (DDoS) protection. [See [Understanding Distributed Denial-of-Service Protection on QFX Series Switches](#).]
- Unified Forwarding Table (UFT). [See [Understanding the Unified Forwarding Table](#).]

Interfaces and Chassis

- **Multichassis link aggregation groups, configuration synchronization, and configuration consistency check (MC-LAG) (QFX5120 switches)**—Starting in Junos OS Release 19.1R1, MC-LAG enables a client device to form a logical LAG interface using two switches. MC-LAG provides redundancy and load balancing between the two switches, multihoming support, and a loop-free Layer 2 network without running spanning tree protocols (STP).

[See [Multichassis Link Aggregation Features, Terms, and Best Practices](#).]

- **Increasing the number of ARP and neighbor discovery entries to 256,000 (QFX10008 and QFX10016 switches)**—Starting in Junos OS Release 19.1R1, the number of ARP and neighbor discovery entries has increased to 256,000 when enabling the **enhanced-convergence** statement. Enhanced convergence improves Layer 2 and Layer 3 convergence time during enhanced MC-LAG and VXLAN L3 gateway restoration scenarios.

To increase the number of ARP and neighbor discovery entries, enable the **arp-enhanced-scale** statement at the **[edit system]** hierarchy.

[See [Increasing ARP and Network Discovery Protocol Entries for Enhanced MC-LAG and Layer 3 VXLAN Topologies](#).]

- **Channelizing enhancement on QFX5210-64C switches**—Starting in Junos OS Release 19.1R1, the behavior of Flexi-pic mode on QFX5210-64C switches has improved. Channelizing ports in this mode no longer disables a corresponding port. The new behavior allows you to use any port within four designated blocks for channelization as long as the total number of channels does not exceed 128 or 32 in any one of the four blocks. Channelization helps to maximize port utilization.

[See [Channelizing Interfaces on Switches](#).]

- **Channelizing interfaces on QFX5120-32C switches**—The 32 ports on the QFX5120-32C switch support native 40- or 100-Gigabit Ethernet configuration and channelized 10-, 25-, or 40-Gigabit Ethernet configuration. Starting in Junos OS Release 19.1R1, you can channelize the default 100-Gbps ports into four 25-Gigabit Ethernet or two 50-Gigabit Ethernet interfaces, and the 40-Gbps ports into four 10-Gigabit Ethernet interfaces (using breakout cables).

If you have disabled auto-channelization, then to channelize the ports, manually configure the port speed using the **set chassis fpc slot-number port port-number channel-speed speed** command, where the speed can be set to **10G, 25G, 50G**.

NOTE:

- The last 100-Gbps port (port 31) does not support four 10-Gigabit Ethernet port or four 25-Gigabit Ethernet port channelization. Only 40-Gigabit Ethernet, 100-Gigabit Ethernet and 2x50-Gigabit Ethernet interfaces are supported on port 31.
- You cannot configure channelized interfaces to operate as Virtual Chassis ports.

[See [Channelizing Interfaces on Switches](#).]

Junos Telemetry Interface

- **Support for the Junos Telemetry Interface (JTI) (QFX10002 and PTX10002)**—Starting with Junos OS Release 19.1R1, you can provision sensors through the Junos Telemetry Interface to export telemetry data for several network elements without involving polling. You can stream data through UDP or gRPC.

Only the following sensors are supported on QFX10002 switches and PTX10002 routers:

- Physical interfaces statistics
- Label-switched-path (LSP) statistics
- Network processing unit (NPU) memory
- NPU memory utilization
- CPU memory

To provision sensors to stream data through UDP, all parameters are configured at the **[edit services analytics]** hierarchy level.

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

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

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

Layer 2 Features

- **L2PT support (QFX5200 switches and QFX5200 Virtual Chassis)**—Starting with Junos OS Release 19.1R1, you can configure Layer 2 protocol tunneling (L2PT) for the following protocols on QFX5200 switches and QFX5200 Virtual Chassis: CDP, E-LMI, GVRP, IEEE 802.1X, IEEE 802.3AH, LACP, LLDP, MMRP, MVRP, STP (including RSTP and MSTP), UDLD, VSTP, and VTP.

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

Licensing

- **QFX5120-32C switch license** —Starting in Junos OS Release 19.1R1, Juniper Networks introduces the QFX5120-32C switch.

The QFX5120-32C switch supports the following licenses models:

- Base features for the QFX5120-32C switch include OSPF, OSPFv3, and RIPng.
- Advanced Feature License (AFL) for QFX5120-32C switch includes BGP, IS-IS, MPLS, VXLAN, and Open vSwitch Database (OVSDB).
- PFL for QFX5120-32C switch includes Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB).

[See [Software Features That Require Licenses for QFX Series](#).]

Management

- **Tracing support for individual JET application files (QFX Series)**—Previously you could configure traceoptions for all applications. Starting in Junos OS Release 19.1R1, you can also configure traceoptions for an individual application file. If you configure trace options both globally (all applications) and locally (by application file), the local configuration has the higher priority. You must commit global traceoptions and the daemonized application configurations at the same time for the global traceoptions for the daemonized application to take effect.

[See [application](#).]

MPLS

- **MPLS scaling enhancements (QFX5100, QFX5110, QFX5200, QFX5210)**—Starting in Junos OS Release 19.1R1, MPLS scaling is enhanced on the switches. For instance, you can increase the scale from its default 1024 to 8192 on the QFX5100. This enhancement optimizes and increases the ingress tunnel scale to address the current needs of data center networks either in IP-CLOS or IP over MPLS application spaces.

[See [Supported MPLS Scaling Values](#).]

- **Use of SID labels as first hop for resolving non-colored static segment routing LSPs (QFX Series)**—Currently, for a static non-colored segment routing traffic-engineered LSP to be usable, the first hop of the segment list must be an IP address. Only the second to *n*th hop could be segment identifier (SID) labels. Starting in Junos OS Release 19.1R1, this requirement does not apply. You can now configure SID labels as the first hop in the segment list.

With this configuration, static non-colored segment routing LSPs are resolved using MPLS fast reroute (FRR) and weighted equal-cost multipath. Without this configuration, by default, the LSPs are resolved using IP address.

[See [Static Segment Routing Label Switched Path](#).]

- **Support of install statement for segment routing LSPs (QFX Series)**—The *install destination-prefix* statement which is currently supported at the `[edit protocols mpls label-switched-path lsp-name]` and `[edit protocols mpls static-label-switched-path lsp-name ingress]` hierarchy levels is now also supported at the `[edit protocols source-packet-routing source-routing-path lsp-name]` hierarchy level for both colored and non-colored static segment routing label-switched paths (LSPs).

You can associate one or more prefixes with a segment routing LSP using the **install** statement. When the LSP is up, all the prefixes are installed as entries into the **inet.3** or **inet6.3** routing table.

[See [install \(Protocols MPLS\)](#).]

- **Control transport address used for targeted-LDP session (QFX Series)**—Currently, only the router-ID or interface address is used as the LDP transport address. Starting in Junos OS Release 19.1R1, you can configure any other IP address as the transport address of targeted LDP sessions, session-groups, and interfaces. This new configuration is applicable only for configured LDP neighbors that have Layer 2 circuit, MPLS, and VPLS adjacencies.

This feature is beneficial when you have multiple loopback interface addresses, and different IGPs associated with LDP interfaces, and you can control the session established between targeted LDP neighbors with the configured transport address.

[See [Control Transport Address Used for Targeted-LDP Session](#).]

- **Policy-based multipath routes (QFX Series)**—In segment routing networks with multiple protocols in the core, you can combine segment routing traffic-engineered (SR-TE) LDP routes and SR-TE IP routes to create a multipath route that is installed in the routing information base (also known as routing table). You can resolve BGP service routes over the multipath route through policy configuration and steer traffic differently for different prefixes.

[See [Policy-Based Multipath Routes Overview](#).]

Network Management and Monitoring

- **Local port mirroring support (QFX10002-60C switch)**—Starting in Junos OS Release 19.1R1, QFX10002-60C switches support local 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.

[See [Examples: Configuring Port Mirroring for Local Analysis](#).]

- **sFlow performance improvements (QFX Series)**—Starting in Junos OS Release 19.1R1, the following improvements have been added to the sFlow technology feature:
 - For MX Series, PTX Series, and QFX Series, you can configure forwarding class and DSCP values per collector.
 - For PTX Series and QFX Series, you can configure IPv6 addresses for the **source-ip** and **agent-id**.
 - Enhancements are made to the following CLI commands: **show sflow collector**, **show sflow collector address ip-address**, and **show sflow interface**.

[See [Understanding How to Use sFlow Technology for Network Monitoring](#), [collector](#), [agent-id](#), [source-ip](#), [show flow collector](#), and [show flow interface](#).]

Routing Policy and Firewall Filters

- **Support for IPv6 filter-based forwarding (QFX5100, QFX5110, and QFX5200 switches)**— Starting with Junos OS Release 19.1R1, you can use stateless firewall filters in conjunction with filters and routing instances to control how IPv6 traffic travels in a network. This is called IPv6 filter-based forwarding. To set up this feature, you define a filtering term that matches incoming packets based on the source or destination address and then specify the routing instance to send packets to. You can use filter-based forwarding to route specific types of traffic through a firewall or security device before the traffic continues on its path. You can also use it to give certain types of traffic preferential treatment or to improve load balancing of switch traffic.

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

[See [Firewall Filter Match Conditions](#) and [Understanding Filter-Based Forwarding](#).]

- **Support for 2000 Egress Firewall Filters (QFX5110 switches)**—Starting in Junos OS Release 19.1R1, you can configure up to 2000 VLAN firewall filters on the switch. This feature is only supported in the egress direction (traffic exiting the VLAN). To configure, include the **egress-to-ingress** option under the **from** statement at the **[edit firewall]** hierarchy level.

[See [Planning the Number of Firewall Filters to Create](#).]

- **Support for packet load balancing based on GTP-TEID hashing (QFX10002, QFX10008, and QFX10016 switches)**—Starting in Junos OS Release 19.1R1, you can configure load balancing of IPv4 or IPv6 packets by using GPRS Tunneling Protocol-tunnel endpoint identifier (GTP-TEID) field hash calculations. The GTP-TEID hashing is added to the Layer 2 and Layer 3 field hashing that you have already configured. To enable this feature, configure the **gtp-tunnel-endpoint-identifier** statement at the **[edit forwarding-options enhanced-hash-key family inet]** or the **[edit forwarding-options enhanced-hash-key family inet6]** hierarchy Level. GTP versions 1 and 2 are supported; they support only user data. You must use UDP port number 2152 for both GTP versions.

[See [gtp-tunnel-endpoint-identifier](#).]

- **Support for matching IPv6 source addresses from an inet6 egress interface (QFX5100)**—Starting in Junos OS Release 19.1R1, you can configure an firewall filter on a IPv6 egress interface to match specified IPv6 source or destination addresses, for example, to protect a third-party device connected to the switch.

[See [eracl-ip6-match](#) and [Example: Configuring an Egress Filter Based on IPv6 Source or Destination IP Addresses](#).]

Routing Protocols

- **Support for BGP graceful shutdown (QFX Series)**— Starting in Junos OS Release 19.1R1, graceful traffic migration from one BGP next hop to another is supported, without traffic interruption. Also, BGP administrative shutdown communication can be sent to the BGP peer.

You can configure both **graceful-shutdown** and **shutdown** statements at the **[edit protocols bgp]**, **[edit protocols bgp group *group-name*]**, and **[edit protocols bgp group *group-name* neighbor *address*]** hierarchy levels.

NOTE: Graceful shutdown is disabled by default.

[See: [graceful-shutdown \(Protocols BGP\)](#), [shutdown \(Protocols BGP\)](#).]

- **Support for 128 equal-cost paths for BGP multipath (QFX10000)**—Starting with Junos OS Release 19.1R1, 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](#).]

- **Support for policy-based allocation for IPv4 BGP-labeled unicast (QFX Series)**—Starting in Junos OS Release 19.1R1, this feature supports:
 - Allocating policy-based label for IPv4 BGP-LU prefixes in per-prefix label allocation mode.
 - 1:1 mapping between prefixes and labels.
 - Map policy for labels.
 - Fallback actions of dynamic and reject for handling error conditions.

[See [policy-options](#), [route-filter-list](#).]

System Management

- **Support for aggregated Ethernet and loopback interfaces on masters and slaves using PTP (QFX5110 switches)** —Starting with Junos OS Release 19.1R1, you can configure both primary and secondary interfaces as aggregated Ethernet and loopback interfaces using PTP over IPv4 and IPv6 unicast transport on the IEEE 1588v2 default profile and the G.8275.2 enhanced profile. Although, the loopback interface (lo0.0) is the same for both the primary and secondary aggregated Ethernet interfaces, the IP addresses must be unique.

[See [Understanding the PTP G.8275.2 Enhanced Profile \(Telecom Profile\)Multicast Overview.](#)]

SEE ALSO

[Changes in Behavior and Syntax | 184](#)

[Known Behavior | 187](#)

[Known Issues | 189](#)

[Resolved Issues | 195](#)

[Documentation Updates | 200](#)

[Migration, Upgrade, and Downgrade Instructions | 201](#)

[Product Compatibility | 215](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [Interfaces and Chassis | 185](#)
- [Network Management and Monitoring | 186](#)
- [Security | 186](#)
- [User Interface and Configuration | 186](#)

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 19.1R1 for the QFX Series.

Interfaces and Chassis

- **Commit error thrown when GRE interface and tunnel source interface configured in different routing instances (QFX Series)**—In Junos OS Release 19.1R1, QFX Series switches does not support configuring GRE interface and the underlying tunnel source interface in two different routing instances. If you try this configuration, it will result in a commit error with the following error message:

error: GRE interface (gr-0/0/0.0) and its underlying tunnel source interface are in different routing-instances

error: configuration check-out failed

[See [Understanding Generic Routing Encapsulation](#).]

- **New XML tag element <lacp-hold-up-state> added in show lacp interfaces XML display (QFX Series)**—Starting in Junos OS Release 19.1R1, the `show lacp interfaces | display xml` command displays a new XML tag element <lacp-hold-up-state>. The <lacp-hold-up-state> displays the time interval an interface holds before it changes from state, down to up. In earlier Junos OS releases, the LACP hold up the information for all interfaces were in a single <lacp-hold-up-information> XML tag. Now, for each interface it is displayed in a separate <lacp-hold-up-information> XML tag.
- **Support for creating Layer 2 logical interfaces independently (QFX Series)**—In Junos OS Releases 18.4R1, 18.4R2, 19.1R1, 19.1R2, and later, QFX Series switches support creating Layer 2 logical interfaces independent of Layer 2 routing instance type. That is, you can configure and commit the Layer 2 logical interfaces separately and add the interface to the bridge domain or Ethernet VPN (EVPN) routing instance separately. Note that the Layer 2 logical interfaces works fine only when the interface is added to the bridge domain or EVPN routing instance.

In the earlier Junos OS releases, when a Layer 2 logical interface configuration (units with encapsulation vlan-bridge configuration) is used, then the logical interface must be added as part of a bridge-domain or EVPN routing instance for the commit to succeed.

Network Management and Monitoring

- **NETCONF <kill-session> operation returns different values in <rpc-error> when the session identifier is equal to the current session ID (QFX Series)**—Starting in Junos OS Release 19.1R1, when you execute the <kill-session> NETCONF operation and the session identifier is equal to the current session ID, the values of the <error-type> and <error-tag> elements in the resulting <rpc-error> are **application** and **invalid-value**, respectively. In earlier releases, the <error-type> and <error-tag> values are **protocol** and **operation-failed**.

[See [<kill-session>](#).]

Security

- **Syslog or log action on firewall drops packets (QFX5000 switches)**—Starting in 19.1R1, if you configure a syslog or log action on an ingress firewall filter, control packets and ICMP packets sent to the Routing Engine might be dropped.
- **Firewall warning message (QFX5000 switches)**—Starting in 19.1R1, a warning message is displayed whenever a firewall term includes log or syslog with the accept filter action.

User Interface and Configuration

- **Options for monitor traffic interfaces statement added (QFX Series)**—Starting in Junos OS Release 19.1R1, the options **write-file** and **read-file** under the **monitor traffic** command are included in the visible CLI.

[See [monitor traffic](#).]

SEE ALSO

[New and Changed Features | 170](#)

[Known Behavior | 187](#)

[Known Issues | 189](#)

[Resolved Issues | 195](#)

[Documentation Updates | 200](#)

[Migration, Upgrade, and Downgrade Instructions | 201](#)

[Product Compatibility | 215](#)

Known Behavior

IN THIS SECTION

- [EVPN | 187](#)
- [Layer 2 Features | 187](#)
- [MPLS | 188](#)
- [Platform and Infrastructure | 188](#)
- [Routing Protocols | 189](#)
- [Virtual Chassis | 189](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 19.1R1 for the QFX Series.

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

EVPN

- On QFX10000 switches configured as type-5 route peers, when only peer 1 advertises routes, that peer might not install the de-encapsulated next-hop route. As a result, type-5 encapsulated traffic sent by peer 2 is dropped until peer 2 advertises any type-5 route. As a workaround, configure a static route pointing to discard on peer 2 and advertise that route as a type-5 route to peer 1. [PR1191092](#)
- 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](#)
- IRB MAC/IP information will be deleted from Ethernet-switching ARP/ND table when **no-arp-suppression** is configured. [PR1394959](#)

Layer 2 Features

- The **Targeted-broadcast forward-only** command does not broadcast the traffic. [PR1359031](#)
- When there are a large number of vmembers getting added in the system, if space for adding vmembers in the kernel runs out, an error is thrown. On encountering the error, L2ALD stops retrying. As a result, no new vmembers are created. This is only seen in a system with very high scale (example 132,000 vmembers). [PR1408845](#)

- xSTP configuration is not supported on flexible vlan tagging interfaces for any of the QFX5000 line of devices (5100, 5110, 5200, 5210, 5120). [PR1414659](#)

MPLS

- There will not be any warning message about Packet Forwarding Engine restart when MPLS tunnel extend configuration is deleted. [PR1394722](#)

Platform and Infrastructure

- When the sFlow collector can be reached only through the Routing Engine, large samples due to heavy traffic can cause the Routing Engine CPU to become busy. [PR1332337](#)
- On QFX10002, QFX10008, and QFX10016, ND is incorrectly working on IRB/Layer 3 interface with discard filter. [PR1338067](#)
- Hardware watchdog does not work on QFX10008 and QFX10002-60C. [PR1343131](#)
- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter will not be installed. [PR1362609](#)
- On QFX5120 switch with 288,000 MAC scale, Routing Engine **show ethernet-switching table summary** command output shows the learned scale entries after a delay of around 60 seconds. [PR1367538](#)
- Junos OS can hang trying to acquire the SMP IPI lock while rebooting when it is running as a VM on Linux and QEMU hypervisor. Device can be recovered using power-cycle of the device. [PR1385970](#)
- These error logs are expected when routes pointing to target next hops in turn pointing to HOLD next hops. These error logs will appear for a short time. Later, when the next hop changes from HOLD next hop to valid next hop, unicast next hops will be walked again and updated with the appropriate weight and reroute counters, and no more error logs will be seen. [PR1387559](#)
- Re-ARP request sent without VLAN-ID (so Routing Engine-ARP fails). [PR1390794](#)
- The QFX5100 (Junos OS Release 19.1R1 non-TVP) uses SDK version 6.3.7. Unified ISSU with BST configuration is not supported and is a product limitation with regard to BCM chipset running on SDK 6.3.7. Even configuring BST after the unified ISSU might not work. As a workaround, restarting of Packet Forwarding Engine is required after the unified ISSU. For QFX5110, the unified ISSU is not supported on Junos OS Release 19.1R1. [PR1395587](#)
- On QFX5120 system, the hardware link scan thread interrupt processing takes significant time due to firmware limitation. This results in greater than 50ms convergence delay during MPLS FRR. [PR1403082](#)

Routing Protocols

- When an interface is configured with family mpls, one label is reserved for explicit-null case. Only one label is used across the different MPLS interfaces for explicit-null case. This label will only be deleted when all the interfaces with family mpls are deleted. So the maximum number of tunnels you can have is 1. [PR1418733](#)

Virtual Chassis

- A Virtual Chassis internal loop might happen at a node coming up from a reboot. During nonstop software upgrade (NSSU) on a QFX5100 Virtual Chassis, a minimal traffic disruption or traffic loop(>2 seconds) might occur. [PR1347902](#)

SEE ALSO

New and Changed Features	 170
Changes in Behavior and Syntax	 184
Known Issues	 189
Resolved Issues	 195
Documentation Updates	 200
Migration, Upgrade, and Downgrade Instructions	 201
Product Compatibility	 215

Known Issues

IN THIS SECTION

- [EVPN](#) | [190](#)
- [General Routing](#) | [190](#)
- [Layer 2 Features](#) | [191](#)
- [MPLS](#) | [191](#)
- [Platform and Infrastructure](#) | [191](#)
- [Routing Protocols](#) | [194](#)

This section lists the known issues in hardware and software in Junos OS Release 19.1R1 for the QFX Series switches.

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

EVPN

- To filter and see the output of desired ESI or neighbor information of an EVPN instance, we created two new choices, namely **show evpn instance <> esi-info esi <> show evpn instance <> neighbor-info neighbor <>**. [PR1402175](#)
- A ping between IRB interfaces on QFX10000 switches over an EVPN type-5 route does not work. The destination switch receives the ICMP request packet but does not respond. [PR1423928](#)

General Routing

- Interface flap is observed only on peer port 100GBASE-LR4 optics in the warm boot stage of VM's during unified ISSU process. [PR1353415](#)
- When **show** command is taking a long time to display results, the STP might change states as BPDUs are no longer processed and causes lot of outages. [PR1390330](#)
- Sometimes when an FPC is manually toggled offline and online, the traffic might stop getting forwarded on some ports. As a result, BFD sessions might go down. [PR1390389](#)
- Layer 2 multicast and broadcast convergence is high while deleting and adding back the scale configurations of VLANs and VXLAN. [PR1399002](#)
- Maximum egress Layer 3 interfaces that can be configured on QFX5100 and QFX5200 is 8000 each, and QFX5110 is 12000. [PR1406107](#)
- On QFX10002, QFX10008, and QFX10016, a auto correctable non-fatal hardware error on PE chip (which is ASIC on QFX10002 and the line card on QFX10008/QFX10016) is reported as 'FATAL' error. Therefore, the related Packet Forwarding Engine gets disabled. The code changes have been made to change the error category from 'FATAL' to 'INFO' to avoid the Packet Forwarding Engine getting disabled unexpectedly. [PR1408012](#)
- When IPv4 and IPv6 are programmed at the same time, most of the IPv6 routes are not installed because the hardware route table gets full. [PR1412873](#)
- After back to back configuration changes on QFX5000 and EX4300-48MP, EVPN proxy ARP feature might not longer suppress ARP and/or network solicitation. However, IPv4 ARP and IPv6 network delivery (ND) process might still complete with remote destination host. [PR1414698](#)
- The libvirtMib_subagent core file might be generated during the installation of images. As a result, there is no functional impact. [PR1419536](#)

- When a bad Optics is connected to the device that inhibit EEPROM failure conditions or I2C read failure conditions, Fxpc might not come up after connecting Avago qfsp 40G. [PR1420874](#)
- The DHCP binding on client might fail when QFX5120-32C acts as DHCP server. This issue is seen only for channelized port. For nonchannelized port such as 40G or 100G, this issue is not seen. [PR1421110](#)
- BUM traffic coming over IRB underlay interface gets dropped on destination VTEP in PIM based VxLAN. [PR1423705](#)
- EVPN-VXLAN IGMP Snooping immediate leave will continue to forward traffic until group timeout timer expires. [PR1424969](#)
- After NSSU, the lag ports stuck in detached state can be recovered by deactivating/activating the lag interface. [PR1425441](#)

Layer 2 Features

- In case of the access side interfaces used as SP style interfaces, when a new logical interface is added and if there is already a logical interface on the physical interface, there is a 20-50 msec traffic drop on the existing logical interface. [PR1367488](#)

MPLS

- There could be some lingering RSVP state that would keep some labeled routes programmed in the Packet Forwarding Engine longer than they should be. This RSVP state will eventually expire and then delete the RSVP MPLS routes from FIB. However, traffic losses is not anticipated due to this lingering state or the corresponding label routes in the FIB. In the worst case, in a network where there is persistent link flapping going on, this lingering state could interfere with the LSP scale being achieved. [PR1331976](#)

Platform and Infrastructure

- In configurations with IRB interfaces, during times of interface deletion (for example, FPC reboot), the Packet Forwarding Engine might log errors stating **nh_ucast_change:291Referenced l2ifl not found**. This condition should be transient, with the system reconverging on the expected state. [PR1054798](#)
- L3 multicast traffic does not converge to 100 percentage and continuous drops are observed after bringing down/up the downstream interface or while an FPC comes online after FPC restart. This happens with multicast replication for 1000 VLAN/IRBs. [PR1161485](#)
- Port LEDs on QFX5100 do not work. If a device connects to a port on QFX5100, the port LED stays unlit. [PR1317750](#)
- QFX10000 platform drops the Aruba wireless Access Point (AP) heartbeat packets. As a result, the Aruba wireless AP cannot work. [PR1352805](#)

- When rpd reads next hops from the kernel on restart, for INH -> FWD NH{List NH} -> {Chain NH} scenario, rpd should not create an old-style list next hop for the forwarding next hop. [PR1360354](#)
- On the QFX5100, if a scaled configuration involving a LAG interface, more than 3000 VLANs, and corresponding next hops is removed and a new configuration involving a LAG interface is applied at the same time, the new configuration might not take effect until the previous configuration has been deleted. During this time, FXPC might take high CPU resources. No other system impact is observed. [PR1363896](#)
- QFX52100: Filter with then routing-instance applied to family inet logical interface causes traffic to be discarded on unrelated interfaces. [PR1364020](#)
- The time lapse between interface-down interrupt detection to FRR callback is approximately 148 ms on the QFX5120 platform, though the in-place update FRR programming completes in 1 ms. The minimum FRR time achieved with this limitation is approximately 150 ms and maximum is approximately 275 ms. [PR1364244](#)
- The statement `pm4x25_line_side_phymod_interfa` might throw the error **ERROR: u=0 p=81 interface type 16 not supported by internal SERDES for this speed 50000**. This error message is seen when channelization is detected in the build 18.1R3. [PR1366137](#)
- On the QFX10000 line of switches, with EVPN-VXLAN, the following error is seen:
`expr_nh_fwd_get_egress_install_mask:nh type Indirect of nh_id: # is invalid`. [PR1367121](#)
- USB upgrade of NOS image is not supported. [PR1373900](#)
- 1.Ingress VLAN mirroring is supported only using the analyzer stanza and does not work with a firewall-based configuration. 2.Ingress VLAN mirroring is not supported with other firewall filters using VLAN on which VXLAN enabled as a match condition. 3.Ingress vlan mirroring has to be configured again if the VLANs are deleted or the EVPN-VXLAN configuration is deleted. [PR1384732](#)
- On QFX10008 and QFX10016 platforms, traffic loss might be observed because of switch modular failure on the Control Board (CB). This failure further causes all SIBs to be marked as faulty and causes FPCs to restart until Routing Engine switchover occurs. [PR1384870](#)
- In rare cases, rpd could end up with stuck KRT queue entries (visible in `show krt queue` output) as a result of interface flaps when using VRF configurations along with a static default route to em0.0 interface. [PR1386475](#)
- Cpsm (control plane switch management) daemon memory leak occurs in VMHOST, it might and the logrotate utility might not work, resulting in cpsm log size. [PR1387903](#)
- On QFX5100 Virtual Chassis, ARP received on SP-Style interface is not sent to all RVTEPs. Normal BUM traffic works fine. [PR1388811](#)
- On QFX10000 switches, the major alarm **FPC Management Ethernet Link Down** might be displayed for management Ethernet (em0 or em1) interface that is administratively down. The alarm message has no service impact and can be ignored. [PR1391949](#)
- DCPFE didn't come up in some instances of abrupt power-off/power-on of QFX5120/EX4650. Power-cycle of the device or host reboot will recover the device. [PR1393554](#)

- On QFX5100, traffic initiated from a server connected to an interface will be dropped at the interface on the switch if the interface was configured with family Ethernet-switching with VXLAN and the configuration is changed to family inet. [PR1399733](#)
- On QFX5110 platforms, from Junos 17.3 OS Release onwards, the interfaces with SFP-LX10 transceivers and auto negotiation enabled (default configuration) might be down. [PR1399878](#)
- Below error logs might be seen when GRE tunneling is configured:
0:_bcm_esw_stat_flex_attach_ingress_table_counters1: Table:VLAN Has already allocated with index:4094base 48 mode 1.First dealloc it. It does not affect the functionality. [PR1400515](#)
- QFX5120: OVSDB-managed VXLAN sees traffic loss. [PR1401943](#)
- USB install: If USB is not removed from device after USB upgrade, the system won't come up and it will keep rebooting. You must manually change the boot sequence from BIOS menu to select boot from SSD. PXE install: The system boots twice from PXE before booting from SSD. This increases boot time. [PR1404717](#)
- Transition from collapsed to non-collapsed L2/L3 GW and vice versa needs switch reload due to stale source VTEP IP. [PR1405956](#)
- There is a possibility of seeing multiple reconnect logs, JTASK_IO_CONNECT_FAILED, during the device initialization. There is no functionality impact due to these messages. These messages can be ignored. [PR1408995](#)
- On QFX10008/10016 platforms, when the FPC come online after a restart, the intra-VLAN traffic ingressing on the aggregated Ethernet interface might be permanently lost if MC-LAG enhanced-convergence is configured and there is only one member link in MC-LAG on the other FPC. [PR1409631](#)
- When using PSM4 optics on QFX5120, there is a possibility that due to a timing fault on FPGA hardware, link might go down due to tx laser being disabled and require administratively toggling the link to enable it back. [PR1410687](#)
- Intermittently, chassis alarms are not raised after power-cycle of the device. Chassis alarms can be recovered by restarting lcmd from the CLI using - **request app-engine service restart chassis-manager** or **restart chassis-control**. [PR1413981](#)
- During BGP flap, route delete and route add request to rpd might get compressed, which results in VXLAN database not getting updated with the correct unicast next hop to stitch it with VENH. So VENH will not have a unicast next hop to forward the traffic. This can be seen using nhinfo in kernel or **show nhdb id <> recursive** in FPC VTY. [PR1415450](#)
- FEC change from FEC91 to NONE is not taking effect on 100-Gigabit Ethernet interfaces with QSFP-100GBASE-SR4 optics. [PR1416376](#)
- On QFX 5110, QFX 5120 platforms, uRPF check in strict mode will not work properly. [PR1417546](#)
- On repeated power cycle tests, it is observed that randomly some 100-Gigabit Ethernet links take longer to link up. Due to this issue, if specific speed is not configured using **set chassis fpc 0 pic 0 port <> speed**

<> configuration, auto-channelization can kick in after 40 seconds of the link remaining in down state, and hence channelize the port. [PR1417622](#)

- During repeated power cycle tests, occasionally it is observed that 100G PSM4 optics go to a state where link does not come up. This issue happens more frequently in a negative temperature environment (below -5 degrees Celsius). Physically resetting the transceiver or power cycling the device will help recover from issue state. [PR1419826](#)
- Traffic drop might be observed when transit static LSP is configured on EX4650 and QFX5120 platforms. [PR1420370](#)

Routing Protocols

- Higher convergence time for LFA with BFD occurs in the Junos OS Release 18.1. [PR1337412](#)
- On QFX Series platforms, in a corner scenario with a Virtual Chassis setup, if storm control configuration is enabled on interfaces and multicast traffic ingresses on the interfaces, some storm control error logs might be observed on these interfaces. It is only seen in one customer setup and not reproducible in a local setup. Also, it is just a logging issue and has no traffic impact. [PR1355607](#)
- On a scaled setup, when the host table is full and the host entries are installed in the LPM table, OSPF sessions might take more time to come up. [PR1358289](#)
- With multicast traffic enabled, multicast counters statistics creation or deletion fails and the following errors might occur during LAG member enable/disable on QFX51xx, QFX52xx devices. The messages do not indicate traffic impact. However, multicast statistics will not work when these messages are seen.
Feb 15 07:28:49 switch fpc0 brcm_ipmc_get_multicast_stats:3947 brcm_ipmc_stat_get failure Feb 15 07:28:49 switch fpc0 brcm_rt_stats:1906 brcm_ipmc_get_multicast_stats failure err=-7. [PR1392470](#)
- AUTONEG errors and flush operation failed error are seen after power cycle of the device. These error messages do not have any functionality impact: **LOG: Err] ifd 153; Ether autonegotiation error (1000) and ch_vchassis_ipc_flush_pipe: flush operation failed for pipe 155333280.** [PR1394866](#)
- When a MOLEX QSFP+ DAC cable is connected to the QFX5210, the link will not come up. A DCPFE generate a core file and the fxpc process will not come up. [PR1397158](#)
- There is no functionality impact due to this error message: **Error BRCM_NH-,brcm_nh_bdvlan_ucast_uninstall(),128:l3 nh 6594 uninstall failed.** [PR1407175](#)
- The separate group creation for egress-to-ingress feature (in QFX5110) is supported from Junos OS 19.1R1 later releases. In Junos OS Release 19.1R1, this feature uses the already existing ERACL firewall group. As a result, extra qualifier in ERACL group operates in double wide mode instead of single wide leading to reduced scale. [PR1408670](#)

SEE ALSO

New and Changed Features	170
Changes in Behavior and Syntax	184
Known Behavior	187
Resolved Issues	195
Documentation Updates	200
Migration, Upgrade, and Downgrade Instructions	201
Product Compatibility	215

Resolved Issues

IN THIS SECTION

- [EVPN | 195](#)
- [Interfaces and Chassis | 196](#)
- [Layer 2 Ethernet Services | 196](#)
- [Layer 2 Features | 196](#)
- [MPLS | 197](#)
- [Network Management and Monitoring | 197](#)
- [Platform and Infrastructure | 197](#)
- [Routing Protocols | 200](#)

This section lists the issues fixed in Junos OS Release 19.1R1 for the QFX Series.

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

EVPN

- A few minutes of traffic loss might be observed during recovery from link failure. [PR1396597](#)
- VNI is not updated on default route 0.0.0.0/0 advertised by EVPN type 5 prefix when the local is configuration changed. [PR1396915](#)
- EVPN routes might show **Route Label: 0** in addition to the real label. [PR1405695](#)
- The rpd might crash after NSR switchover. [PR1408749](#)

Interfaces and Chassis

- Constant dcpfe process crash might be seen if using an unsupported GRE interface configuration. [PR1369757](#)

Layer 2 Ethernet Services

- After GRES switchover, LACP will be down on the peer device and never recover automatically. [PR1395943](#)

Layer 2 Features

- The IPv6 NS/NA packets coming from the remote VTEP are not getting forwarded to the local host. [PR1387519](#)
- The dcpfe process might crash after VXLAN overlay ping. [PR1388103](#)
- With IGMP snooping enabled on the leaf switches, multicast traffic is forwarded to VLAN/VNI, which doesn't have an active receiver. [PR1388888](#)
- RTG MAC refresh packets will be sent out from non-RTG ports if the RTG interface belonging to the Virtual Chassis master flaps. [PR1389695](#)
- Packets destined to 01:00:0c:cc:cc:cc are not forwarded on QFX10000. [PR1389829](#)
- EVPN-VXLAN: Dcpfe is restarted at the _bcm_field_td_counter_last_hw_val_update routine after upgrading spine with latest image. [PR1398251](#)
- On QFX5000, dcpfe process crash might be observed during restart of Packet Forwarding Engine or system with scaled EVPN/VXLAN configuration. [PR1403305](#)
- The IPv6 NS/NA packets received over VTEP from an ESI host are incorrectly flooded back to the host. [PR1405820](#)
- With Junos OS releases before 19.1R1, on devices with cut-through configuration enabled, after reboot of the device, cut-through mode will be disabled on the channelized interfaces. [PR1407706](#)
- With arp-suppression/proxy-arp feature, QFX5100 or QFX5110 might not forward IPv6 Router Solicitations or Advertisements. [PR1414496](#)

MPLS

- LSP "statistics" and "auto-bandwidth" functionality might not take effect with single-hop LSPs. [PR1390445](#)

Network Management and Monitoring

- Log files might not get compressed during the upgrade. [PR1414303](#)

Platform and Infrastructure

- The 1-Gigabit Ethernet copper module interface shows "Link-mode: Half-duplex" on QFX10000 line platforms. [PR1286709](#)
- Optics BiDi: FEC incorrectly displayed on QFX5110 and QFX10002-36Q. [PR1360948](#)
- SFP-T might not work on QFX5100/QFX5110 devices. [PR1366218](#)
- The first 2 characters out of 14 of AS7816-64 serial number is truncated. [PR1371126](#)
- For the Junos OS 18.1R1 or later, USB image installation on QFX5210-64C, an AMI BIOS upgrade is required. [PR1371199](#)
- Packet Forwarding Engine is in a bad state after performing optics insertion or removal on a port. [PR1372041](#)
- The IPv6 routed packet might be transmitted through an interface whose VRRP state is in non-master. [PR1372163](#)
- QFX5110 ethernet-switching flood group shows incorrect information. [PR1374436](#)
- Packet Forwarding Engine wedge might be observed if there are interfaces going to the down state. [PR1376366](#)
- EM policy update is needed on QFX5210-64C. [PR1380077](#)
- The overlay ECMP might not work as expected on QFX5110 in an EVPN-VXLAN environment. [PR1380084](#)
- IPv6 ping might fail for spine node in EVPN scenario. [PR1380590](#)
- Traffic black hole is caused by FPC offline in MC-LAG scenario. [PR1381446](#)
- The QFX-QSFP-40G-SR4 transceiver might not be recognized after upgrading Junos OS on QFX5100e. [PR1381545](#)
- LACP gets stuck in detached/attached state when the interface is configured with native VLAN ID and VXLAN VLAN. [PR1382209](#)
- QFX10008 continuously shows `RPD_KRT_Q_RETRIES: list nexthop ADD: No such file or directory`. [PR1383426](#)

- The DMA failure errors might be seen when the cache is flushed or the cache is full. [PR1383608](#)
- DHCP packets might be dropped on a Junos Fusion Data Center scenario (QFX10000 line of devices). [PR1383623](#)
- Last reboot reason is not correct if device is rebooted because of power cycle. [PR1383693](#)
- The Virtual Chassis could not come up after upgrading to QFX5E platforms (TVP-based platforms for QFX5100 or QFX5200 switches). [PR1383876](#)
- A “force host” upgrade is required for QFX5110-48S-4C in Junos OS Release 18.4 if the PTP over IPV6 G.8275.2 feature is configured. [PR1384073](#)
- Tuning issue exist for SFPP-10G-DT-ZRC2 and SFPP-10G-CT50-ZR. [PR1384524](#)
- QFX5120: Occasionally two of the channelized 25-Gigabit Ethernet ports using 4x25G breakout cable will not come up after Junos OS reboot. [PR1384898](#)
- The IPv6 packet might not be routed when the IPv6 packet is encapsulated over IPv4 GRE tunnel on QFX10000. [PR1385723](#)
- The spine EVPN routes might be stuck in a hidden state with next hop as unusable after FPC is offline in the spine. [PR1386147](#)
- DDoS statistics and logging are not working for internal queues such as Q42 and Q4. [PR1387508](#)
- Traffic drop might be seen on QFX10000 platform with EVPN-VXLAN configured. [PR1387593](#)
- QFX5100/QFX5110/QFX5200/QFX5210 Virtual Chassis could not be formed normally. [PR1387730](#)
- Certain log messages might be observed on QFX Series platforms. [PR1388479](#)
- MAC learning might stop working on some LAG interfaces. [PR1389411](#)
- FPC might crash on QFX5100 and EX4600 platforms in a large-scale scenario. [PR1389872](#)
- The vmcore might be seen when routing changes are made on the peer spine in an EVPN VXLAN scenario. [PR1390573](#)
- An incorrect error message might be seen when J-Flow sensors are configured with reporting rate less than 30 seconds. [PR1390740](#)
- Smid core file is seen during sanity script execution on QFX5100 and EX4300. [PR1391909](#)
- Sdk-vmmd might consistently write to the memory. [PR1393044](#)
- 10-Gigabit Ethernet copper link flapping might happen during TISSU operation of QFX5100-48T switches. [PR1393628](#)
- IPV6 next-hop programming issue might be observed on QFX10000/PTX1000/PTX10000 devices. [PR1393937](#)
- L2ALD core file is seen when l2-learning traceoptions were enabled. [PR1394380](#)
- DRAM and buffer utilization fields are not correct for QFX10000 platforms. [PR1394978](#)
- PTP over Ethernet traffic could be dropped if IGMP and PTP TC are configured together. [PR1395186](#)

- DOT1XD core found at `pnac_bd_create_pnac_bdm_handler_knl_async_receive_and_process`. [PR1395384](#)
- Unable to install licenses automatically on QFX Series platforms. [PR1395534](#)
- `BRCM_NH-,brcm_bcm_mpls_tunnel_initiator_clear(),226:bcm_mpls_tunnel_initiator_get` failed intf = 4 failure error logs might seen in syslog. [PR1396014](#)
- If GRES/NSR is enabled on a QFX5100 (single Routing Engine), DHCP subscribers are failing to bind. [PR1396470](#)
- QFX10002-60C: FPC might not be detected after the ukern crashes. [PR1396507](#)
- High jsd or na-grpcd CPU usage might be seen even JET or JTI is not used. [PR1398398](#)
- The DHCPv6 relay packets are dropped when both the UDP source and destination ports are 547. [PR1399067](#)
- CPU hog might be observed on QFX10000 platform. [PR1399369](#)
- The DHCPv6 relay-reply packet might be dropped by the DHCP relay. [PR1399683](#)
- ARP refresh functionality might fail in an EVPN scenario. [PR1399873](#)
- PEM I2C failure alarm might be showed incorrectly as failed. [PR1400380](#)
- MAC-limit with persistent MAC is not working after reboot. [PR1400507](#)
- Only one Packet Forwarding Engine could be disabled on FPC with multiple Packet Forwarding Engines in error/wedge condition. [PR1400716](#)
- The authd might crash when issuing **show network-access requests pending** command during the authd restarting. [PR1401249](#)
- File permissions are changed for `/var/db/scripts` files after reboot. [PR1402852](#)
- The VRRP VIP might not work when it is configured on the LAG interface. [PR1404822](#)
- ARP/ND will not be resolved in case of native VLAN ID configured for LAG access interface. [PR1404895](#)
- Commit warning occurs on QFX5100. [PR1405138](#)
- VXLAN transit traffic over tagged underlay L3 Interface gets dropped due to hardware limitation. [PR1406282](#)
- EVPN-VXLAN: QFX10002: With arp-suppression present (enabled by default), packets egressing the QFX Series switch are tagged with 4095 VLAN when using SP-style configurations on the ports. [PR1407059](#)
- DHCP discover packets are getting dropped over VXLAN tunnel on a pure L2 VLAN when DHCP relay is enabled for other VLANs. [PR1408161](#)
- The FPC might crash and could not come up if interface-num or next hop is set to maximum value under vxlan-routing on QFX Series platforms. [PR1409949](#)

Routing Protocols

- QFX5120: The command output **show pfe route summary hw** will show different scale values for the IPv4 and IPv6 LPM routes rather than the supported scale. [PR1366579](#)
- Host-destined packets with filter log action might reach the Routing Engine. [PR1379718](#)
- MMU errors on QFX5200 running Junos OS Release 15.1X53-D234.2. [PR1381790](#)
- BUM packets might get looped if EVPN multihoming interface flaps. [PR1387063](#)
- The next hop in hardware for existing ECMP route might not be updated when **ecmp-resilient-hash** is configured. [PR1387713](#)
- CLI **show evpn igmp-snooping database extensive** output needs to be modified according to the SMET functionality. [PR1391406](#)
- On QFX5110 and QFX5200 switches, the non-collapsed EVPN-VXLAN dcfpe core file is seen at **brcm_pkt_tx_flush, l2alm_mac_ip_timer_handle_expiry_event_loc** after a random event. [PR1397205](#)

SEE ALSO

New and Changed Features 170
Changes in Behavior and Syntax 184
Known Behavior 187
Known Issues 189
Documentation Updates 200
Migration, Upgrade, and Downgrade Instructions 201
Product Compatibility 215

Documentation Updates

There are no errata or changes in Junos OS Release 19.1R1 documentation for the QFX Series.

SEE ALSO

New and Changed Features 170
Changes in Behavior and Syntax 184
Known Behavior 187

[Known Issues | 189](#)

[Resolved Issues | 195](#)

[Migration, Upgrade, and Downgrade Instructions | 201](#)

[Product Compatibility | 215](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrading Software on QFX Series Switches | 201](#)
- [Installing the Software on QFX10002-60C Switches | 204](#)
- [Installing the Software on QFX10002 Switches | 204](#)
- [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 | 205](#)
- [Installing the Software on QFX10008 and QFX10016 Switches | 207](#)
- [Performing a Unified ISSU | 211](#)
- [Preparing the Switch for Software Installation | 212](#)
- [Upgrading the Software Using Unified ISSU | 212](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 214](#)

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

Upgrading Software on QFX Series Switches

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

If you are not familiar with the download and installation process, follow these steps:

1. In a browser, go to <https://www.juniper.net/support/downloads/junos.html>.

The Junos Platforms Download Software page appears.

2. In the QFX Series section of the Junos Platforms Download Software page, select the QFX Series platform for which you want to download the software.
3. Select **18.3** 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 18.3 release.

An Alert box appears.

5. In the Alert box, click the link to the PSN document for details about the software, and click the link to download it.

A login screen appears.

6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Download the software to a local host.
8. Copy the software to the device or to your internal software distribution site.
9. Install the new jinstall package on the device.

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

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

```
user@host> request system software add
source/jinstall-host-qfx-5-x86-64-18.3-R1.n-secure-signed.tgz reboot
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 18.3 **jinstall** package, you can issue the **request system software rollback** command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

This section explains how to upgrade the software, which includes both the host OS and the Junos OS. This upgrade requires that you use a VM host package—for example, a **junos-vmhost-install-x.tgz** .

During a software upgrade, the alternate partition of the SSD is upgraded, which will become primary partition after a reboot .If there is a boot failure on the primary SSD, the switch can boot using the snapshot available on the alternate SSD.

NOTE: The QFX10002-60C switch supports only the 64-bit version of Junos OS.

NOTE: If you have important files in directories other than /config and /var, copy the files to a secure location before upgrading. The files under /config and /var (except /var/etc) are preserved after the upgrade.

To upgrade the software, you can use the following methods:

If the installation package resides locally on the switch, execute the **request vmhost software add <pathname><source>** command.

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-18.1R1.9.tgz
```

If the Install Package resides remotely from the switch, execute the **request vmhost software add <pathname><source>** command.

For example:

```
user@switch> request vmhost software add
ftp://ftpserver/directory/junos-vmhost-install-qfx-x86-64-18.1R1.9.tgz
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Installing the Software on QFX10002 Switches

NOTE: If you are upgrading from a version of software that does not have the FreeBSD 10 kernel (15.1X53-D30, for example), you will need to upgrade from Junos OS Release 15.1X53-D30 to Junos OS Release 15.1X53-D32. After you have installed Junos OS Release 15.1X53-D32, you can upgrade to Junos OS Release 15.1X53-D60 or Junos OS Release 18.3R1.

NOTE: On the switch, use the **force-host** option to force-install the latest version of the Host OS. However, by default, if the Host OS version is different from the one that is already installed on the switch, the latest version is installed without using the **force-host** option.

If the installation package resides locally on the switch, execute the **request system software add <pathname><source> reboot** command.

For example:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-f-x86-64-18.3R1.n-secure-signed.tgz reboot
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> reboot** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-f-x86-64-18.3R1.n-secure-signed.tgz reboot
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at <https://www.juniper.net/support>.

The switch contains two Routing Engines, so you will need to install the software on each Routing Engine (re0 and re1).

If the installation package resides locally on the switch, execute the **request system software add <pathname><source>** command.

To install the software on re0:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> re0** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

To install the software on re1:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> re1** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

Reboot both Routing Engines.

For example:

```
user@switch> request system reboot both-routing-engines
```


After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Installing the Software on QFX10008 and QFX10016 Switches

Because the switch has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at <https://www.juniper.net/support>.



WARNING: If graceful Routing Engine switchover (GRES), nonstop bridging (NSB), or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you issue the CLI **delete chassis redundancy** command when prompted. If GRES is enabled, it will be removed with the **redundancy** command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the **[edit routing-options]** hierarchy level to disable it.

1. Log in to the master Routing Engine's console.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

2. From the command line, enter configuration mode:

```
user@switch> configure
```

3. Disable Routing Engine redundancy:

```
user@switch# delete chassis redundancy
```

4. Disable nonstop-bridging:

```
user@switch# delete protocols layer2-control nonstop-bridging
```

5. Save the configuration change on both Routing Engines:

```
user@switch# commit synchronize
```

6. Exit the CLI configuration mode:

```
user@switch# exit
```

After the switch has been prepared, you first install the new Junos OS release on the backup Routing Engine, while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the software version on the other Routing Engine.

7. Log in to the console port on the other Routing Engine (currently the backup).

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

8. Install the new software package using the **request system software add** command:

```
user@switch> request system software add validate
/var/tmp/jinstall-host-qfx-10-f-x86-64-18.3R1.n-secure-signed.tgz
```

For more information about the **request system software add** command, see the [CLI Explorer](#).

9. Reboot the switch to start the new software using the **request system reboot** command:

```
user@switch> request system reboot
```

NOTE: You must reboot the switch to load the new installation of Junos OS on the switch.

To abort the installation, do not reboot your switch. Instead, finish the installation and then issue the **request system software delete <package-name>** command. This is your last chance to stop the installation.

All the software is loaded when you reboot the switch. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation is not sending traffic.

10. Log in and issue the **show version** command to verify the version of the software installed.

```
user@switch> show version
```

Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the master Routing Engine software.

11. Log in to the master Routing Engine console port.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

12. Transfer routing control to the backup Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the **request chassis routing-engine master** command, see the [CLI Explorer](#).

13. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

```
user@switch> show chassis routing-engine
```

```
Routing Engine status:
Slot 0:
  Current state           Backup
  Election priority       Master (default)
Routing Engine status:
Slot 1:
  Current state           Master
  Election priority       Backup (default)
```

14. Install the new software package using the **request system software add** command:

```
user@switch> request system software add validate
/var/tmp/jinstall-host-qfx-10-f-x86-64-18.3R1.n-secure-signed.tgz
```

For more information about the **request system software add** command, see the [CLI Explorer](#).

15. Reboot the Routing Engine using the **request system reboot** command:

```
user@switch> request system reboot
```

NOTE: You must reboot to load the new installation of Junos OS on the switch.

To abort the installation, do not reboot your system. Instead, finish the installation and then issue the **request system software delete jinstall <package-name>** command. This is your last chance to stop the installation.

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation does not send traffic.

16. Log in and issue the **show version** command to verify the version of the software installed.

17. Transfer routing control back to the master Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the **request chassis routing-engine master** command, see the [CLI Explorer](#).

18. Verify that the master Routing Engine (slot 0) is indeed the master Routing Engine:

```
user@switch> show chassis routing-engine
```

```
Routing Engine status:
  Slot 0:
    Current state           Master
    Election priority       Master (default)
Routing Engine status:
  Slot 1:
    Current state           Backup
    Election priority       Backup (default)
```

Performing a Unified ISSU

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

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

Perform the following tasks:

- [Preparing the Switch for Software Installation on page 212](#)
- [Upgrading the Software Using Unified ISSU on page 212](#)

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

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

To verify that nonstop active routing is enabled:

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

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

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

- Enable nonstop bridging (NSB). See *Configuring Nonstop Bridging on Switches (CLI Procedure)* for information on how to enable it.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the **request system snapshot** command.

Upgrading the Software Using Unified ISSU

This procedure describes how to upgrade the software running on a standalone switch.

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in *Installing Software Packages on QFX Series Devices*.
2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:
 - On the switch, enter:

```
user@switch> request system software in-service-upgrade /var/tmp/package-name.tgz
```

where *package-name.tgz* is, for example, *jinstall-host-qfx-10-f-x86-64-18.3R1.n-secure-signed.tgz*.

NOTE: During the upgrade, you cannot access the Junos OS CLI.

The switch displays status messages similar to the following messages as the upgrade executes:

```
warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get
lost!
ISSU: Validating Image
ISSU: Preparing Backup RE
Prepare for ISSU
ISSU: Backup RE Prepare Done
Extracting jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz ...
Install jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
```

```

ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item          Status          Reason
  FPC 0         Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff

```

NOTE: A unified ISSU might stop, instead of abort, if the FPC is at the warm boot stage. Also, any links that go down and up will not be detected during a warm boot of the Packet Forwarding Engine (PFE).

NOTE: If the unified ISSU process stops, you can look at the log files to diagnose the problem. The log files are located at `/var/log/vjunos-log.tgz`.

5. Log in after the reboot of the switch completes. To verify that the software has been upgraded, enter the following command:

```
user@switch> show version
```

6. Ensure that the resilient dual-root partitions feature operates correctly, by copying the new Junos OS image into the alternate root partitions of all of the switches:

```
user@switch> request system snapshot slice alternate
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases

provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1, 17.2 and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

SEE ALSO

[New and Changed Features | 170](#)

[Changes in Behavior and Syntax | 184](#)

[Known Behavior | 187](#)

[Known Issues | 189](#)

[Resolved Issues | 195](#)

[Documentation Updates | 200](#)

[Product Compatibility | 215](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 215](#)

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://apps.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 170
Changes in Behavior and Syntax 184
Known Behavior 187
Known Issues 189
Resolved Issues 195
Documentation Updates 200
Migration, Upgrade, and Downgrade Instructions 201

Junos OS Release Notes for SRX Series

IN THIS SECTION

- [New and Changed Features | 217](#)
- [Changes in Behavior and Syntax | 229](#)
- [Known Behavior | 231](#)
- [Known Issues | 233](#)
- [Resolved Issues | 235](#)
- [Documentation Updates | 241](#)
- [Migration, Upgrade, and Downgrade Instructions | 242](#)
- [Product Compatibility | 243](#)

These release notes accompany Junos OS Release 19.1R1 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/product/en_US/junos-os.

New and Changed Features

IN THIS SECTION

- Application Security | 218
- Authentication Access Control | 219
- Intrusion Detection and Prevention (IDP) | 219
- J-Web | 220
- Logical Systems and Tenant Systems | 225
- Routing Policy and Firewall Filters | 226
- Routing Protocols | 226
- Security | 226
- Unified Threat Management (UTM) | 226
- VPN | 227

This section describes the new features and enhancements to existing features in Junos OS Release 19.1R1 for the SRX Series devices.

Application Security

- **CLI enhancements to support J-Web in application identification (SRX Series and vSRX)**—Starting in Junos OS Release 19.1R1, the **show services application-identification** command is enhanced to display application and application group details in J-Web.

The **show services application-identification application** command includes the new **risk** option and the **show services application-identification entries** command is enhanced with the new **category-list** and **subcategory-list** options. These options support and improve the J-Web search mechanism.

[See [show services application-identification application](#).]

- **Support for user source identity in APBR policies (SRX Series and vSRX)**—Starting in Junos OS Release 19.1R1, you can configure advanced policy-based routing (APBR) policies by defining the user source identity as one of the match criteria along with source addresses, destination addresses, and applications.

If you specify source identity as a match criteria in a policy, then the user and role information are retrieved before policy lookup can proceed. After a successful match, the APBR profile configured with the APBR policy is used for applying the configured rule.

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

- **Application quality of experience (AppQoE) support in high availability (HA) mode (SRX4100, SRX4200)**—Starting in Junos OS Release 19.1R1, the SRX4100 and SRX4200 support application quality of experience (AppQoE) when these devices operate in chassis cluster mode.

You can configure these SRX Series devices to operate both in active/active and in active/passive modes and deploy the device as spoke device in SD-WAN deployments.

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

- **Application services bypass in APBR (SRX Series and vSRX)**—Starting in Junos OS Release 19.1R1, you can bypass the application services on a session using advanced policy-based routing (APBR) profile rule. When the APBR profile rule is matched and re-routing is done, you can specify that the traffic matching the APBR profile rule can be bypassed from the application services that are configured on the SRX Series devices.

You can use the APBR profile rule to bypass application services such as security policy, application quality of service (AppQoS), Juniper Sky ATP, IDP, Security Intelligence (SecIntel), and UTM using the APBR rule.

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

- **AppQoE scaling support (SRX4100 and SRX4200)**—Starting in Junos OS Release 19.1R1, Application quality of experience (AppQoE) enforces the configuration limit for overlay paths, metric profiles, probe parameters, and SLA rules per profile when you configure application-specific SLA rules and associate the SLA rules to an APBR profile. If you configure more parameters than the allowed limit, an error message is displayed after you commit the configuration.

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

Authentication Access Control

- **Monitoring DHCP session logs (SRX Series)**—Starting in Junos OS Release 19.1R1, you can monitor the Dynamic Host Configuration Protocol (DHCP) session events. Using the session logs generated by the `jdhcp` process, you can observe the session (subscribe) creation, session deletion, and renew events details. You can configure the DHCP session logs by using the `log session` and `log session dhcpv6` options at the `[edit system processes dhcp-service]` hierarchy level for IPv4 and IPv6 addresses, respectively. You can use the session logs for monitoring and troubleshooting purposes.

[See [log](#).]

Intrusion Detection and Prevention (IDP)

- **Covert channels identification and mitigation for IPv6 extension headers (SRX Series and vSRX)**—Starting in Junos OS Release 19.1R1, Intrusion Detection and Prevention (IDP) supports the identification and mitigation of covert channels for IPv6 extension headers.

Covert channel is a type of attack in which information is transferred through existing channels that should not be allowed to communicate by the configured security policy. Thus, this kind of communication violates the existing security system.

The IPv6 covert channel anomalies are part of the IDP signature database package. You can configure the anomalies by using the `predefined-attacks` statement under the `idp-policies` hierarchy level.

[See [Attack Objects and Object Groups for IDP Policies](#).]

- **Deprecation of signatures in IDP (SRX Series and vSRX)**—Starting in Junos OS Release 19.1R1, certain signatures are marked as deprecated or excluded from the Intrusion Prevention System (IPS).

For dynamic attack groups, two filters—`Excluded` and `no-excluded`—are introduced at the `[edit security idp dynamic-attack-group dynamic-attack-group-name filters]` hierarchy level to check the signatures which are part of the database updates.

The `show security idp attack deprecated-list` and `show security idp policy deprecated attacks` commands are introduced to display the list of deprecated attacks in the signature updates.

[See [IDP Signature Database Overview](#).]

- **Support for Hyperscan extended parameters in IDP signature-based attacks (SRX Series and vSRX)**—Starting in Junos OS Release 19.1R1, you can configure signature-based attacks by using Hyperscan extended parameters. By setting optimal values for the Hyperscan extended parameters, you can enhance the attack pattern matching process significantly.

To configure the extended parameters, include the `optional-parameters` option at the `[edit security idp custom-attack attack-name attack-type signature]` hierarchy level. You can configure the following parameters under the `optional-parameters` option:

- `min-offset`

- **max-offset**
- **min-length**

[See [Understanding IDP Signature-Based Attacks.](#)]

J-Web

- **Threat Assessment report supports new charts (SRX Series)**—Starting in Junos OS Release 19.1R1, the Threat Assessment report supports the following charts:
 - Top Web Categories for Security High—Displays only high severities and the top 10 Web categories.
 - Top Web Categories—Displays the top 10 Web categories.
 - Top Users Accessing Risky Websites—Displays the top 10 values.
 - Top URL Categories for Security Risk (High and Medium)—Displays both high and medium severities and the top 10 values.
 - Top URL Categories for Productivity Loss—Displays the top 10 values.
 - Top URL Categories for Legal Liability—Displays the top 10 values.

[See [Reports.](#)]

- **IPsec VPN security services support new authentication algorithm and Diffie-Hellman (DH) group values (SRX Series)**—Starting in Junos OS Release 19.1R1, IPsec VPN security services support and display the following new values:
 - IKE (Phase I)—SHA 512-bit authentication algorithm, DH Group 15, 16, and 21
 - IKE (Phase II)—HMAC-SHA-512 authentication algorithm, HMAC-SHA-384 authentication algorithm, DH Group 15, 16, and 21

NOTE: The new authentication algorithms and DH groups support the SRX5000 line of devices with SPC3 upon installation of junos-ike package only. Click **Install** from **Configure>Security Services>IPsec VPN>Global Settings** to install the package.

[See [VPN Global Settings Configuration Page Options](#), [IKE \(Phase I\) Configuration Page Options](#), and [IKE \(Phase II\) Configuration Page Options](#).]

- **Certificate management supports new bit length for the Elliptic Curve Digital Signature Algorithm (ECDSA) key (SRX Series)**—Starting in Junos OS Release 19.1R1, when you create a certificate, Certificate management supports the bit length of the 521 ECDSA key.

[See [Managing Certificates.](#)]

- **User management supports new password setting range (SRX Series)**—Starting in Junos OS Release 19.1R1, the user management configuration supports the password settings range as follows:
 - Minimum Reuse: 1-20 old passwords, but these must not be the same as the new password you set.
 - Maximum Lifetime: 30-365 days
 - Minimum Lifetime: 1-30 days

NOTE: Using J-Web, you cannot configure the minimum number of characters required for a new password.

[See [User Management Configuration Page Options](#).]

- **In J-Web, device basic settings can be configured on a single page (SRX Series)**—Starting in Junos OS Release 19.1R1, you can configure the following basic settings for a device on a single page in J-Web:
 - System Identity Details
 - Date & Time
 - Management Access Configuration

NOTE: If the SRX Series device does not have a dedicated management port (fxp0), then **Loopback Address** and **Subnet** are the only options available for configuring management access. For SRX Series devices with the fxp0 port, IPv4 configuration is supported for configuring management access.

- Security Logging—Supports only stream mode.
- SNMP

[See [System Identity Configuration Page Options](#).]

- **Support for monitoring logical system users and tenant users (SRX Series)**—Starting in Junos OS Release 19.1R1, the **Users** option under the **Monitor** tab is available for both logical system users and tenant users.

[See [Monitoring Users](#).]

- **Support for events monitoring configuration for logical system users and tenant users (SRX Series)**—Starting in Junos OS Release 19.1R1, the following events monitoring configurations are supported for logical system users and tenant users:
 - Firewall events are supported for both logical system users and tenant users.
 - All events, Web filtering, content filtering, antispam, antivirus, and IPS events are supported for logical system users.

[See [Monitoring Firewall Events](#) and [Monitoring All Events](#).]

- **Supported reports for logical system users and tenant users (SRX1500, SRX4100, SRX4200, and SRX4600)**—Starting in Junos OS Release 19.1R1:
 - Threat assessment, application and user, talkers, firewall, screen, and source zone reports are supported for logical system users and tenant users.
 - IPS, URL, viruses, antispam, Web applications, roles, botnet, malware, blocked application, and permitted application reports are supported only for logical system users.

[See [Reports](#).]

- **Report generation status when the context is switched (SRX Series)**—Starting in Junos OS Release 19.1R1, you can choose to stop generating a report to switch the context or continue generating the report without switching the context using the confirmation message.

[See [Configuring Multi Tenancy Logical Systems](#).]

- **Support for traffic logging (SRX Series)**—Starting in Junos OS Release 19.1R1, traffic logging is enabled as part of the security logging configuration for logical system users and tenant users. When you enable traffic logging, the existing event mode configuration (if any) is deleted.

[See [Security Logging Configuration Page Options](#).]

- **Firewall security policy rules support source identity for local authentication users (SRX Series)**—Starting in Junos OS Release 19.1R1, a list of local authentication users is available in source identity for logical system users and tenant users.

[See [Configuring Firewall Policy Rules](#).]

- **Local authentication monitoring for logical system users and tenant users (SRX Series)**—Starting in Junos OS Release 19.1R1, the local authentication option (Monitor > Authentication > Local Auth) is enabled for logical system and tenant users.

The Clear All option is not available for either logical system users or tenant users to clear the authentication information.

[See [Monitoring Local Authentication](#).]

- **Autocompletion of logical system names or tenant names (SRX Series)**—Starting in Junos OS Release 19.1R1, when you type the partial name of the logical system name or tenant name, the user interface automatically completes the name.

[See [Interconnecting Interface Ports Configuration Page Options](#).]

- **Multitenancy support is provided for logical system users and tenant users (SRX Series)**—Starting in Junos OS Release 19.1R1, you can have the following maximum number of logical system users and tenant users for multitenancy:

Table 2: Maximum Number of Logical System Users and Tenant Users for Multitenancy

SRX Series	Number of Logical System Users	Number of Tenant Users
SRX5000 line of devices with SPC2	32	100
SRX5000 line of devices with SPC3	32	500
SRX5000 line of devices with mixed SPC2 and SPC3	32	100
SRX4600	32	300
SRX4200	32	200
SRX4100	32	200
SRX1500	32	50

[See [Configuring Multi Tenancy Logical Systems](#) and [Configuring Multi Tenancy Tenants](#).]

- **User configurations available on a single page (SRX Series)**—Starting in Junos OS Release 19.1R1, the following user configurations are available on a single page:
 - User Management
 - Firewall Authentication
 - Access Profiles
 - UAC Settings

[See [User Management Configuration Page Options](#).]

- **Address Pool available as a separate configuration page (SRX Series)**—Starting in Junos OS Release 19.1R1, you can access Address Pool as a separate configuration page from Configure > Security Objects.

[See [Address Pools Configuration Page Options](#).]

- **App Tracking available under Security Objects (SRX Series)**—Starting in Junos OS Release 19.1R1, you can configure application tracking from Configure > Security Objects > App Tracking.

[See [Application Tracking Configuration Page Options](#).]

- **Changes on the Monitoring Events page (SRX Series)**—Starting in Junos OS Release 19.1R1, the Summary View is replaced with the Chart View, and the Detailed View is replaced with the Grid View. These changes are applicable to all the configuration pages (except the System page) under Monitor > Events.

[See [Monitoring All Events](#).]

- **IKE (Phase II) supports new values for the Establish tunnels option (SRX Series)**—Starting in Junos OS Release 19.1R1, the Establish tunnels option supports the **responder-only** and **responder-only-no-rekey** values.

NOTE:

- The **responder-only** option is supported on the SRX5000 line of devices with an SPC3 card only if the junos-ike-package is installed. To install this package from J-Web, navigate to **Configure>Security Services>IPsec VPN>Global Settings**, and click **Install**.
- When you configure the **responder-only** value on multiple VPN objects with a single gateway configuration, ensure that all the VPN objects are configured with this mode.
- The **responder-only** option is supported only on a site-to-site VPN. This option is not supported on AutoVPN.

[See [VPN AutoKey Configuration Page Options](#).]

- **New risk values in application signature (SRX Series)**—Starting in Junos OS Release 19.1R1, when the custom application creates an application signature, it supports the following application signature risk levels:
 - Low
 - Moderate
 - Unsafe
 - High
 - Critical

[See [Application Signature Configuration Page Options](#).]

- **Support for PowerMode IPsec (SRX4100, SRX4200, SRX4600, SRX5000 line with SPC3 card, and vSRX)**—Starting in Junos OS Release 19.1R1, you can enable or disable **PowerMode IPsec (PMI)** in the IPsec VPN Global Settings.

NOTE:

- After the PMI configuration is committed, the Packet Forwarding Engine service restarts automatically. The Packet Forwarding Engine service will not be explicitly restarted.
- You can use the J-Web user interface to enable or disable PMI depending on the configuration required for each of the devices.

[See [VPN Global Settings Configuration Page Options](#).]

Logical Systems and Tenant Systems

- **SSL proxy support for logical systems (SRX Series)**—Starting in Junos OS Release 19.1R1, SRX Series devices that have logical systems configured support the Secure Sockets Layer (SSL) proxy functionality. The logical-system users can configure and view the SSL profiles specific to their own logical systems by using the root certificate. The logical-system users can configure SSL profiles for proxy termination and initiation on logical systems and can also configure the certificate authority (CA), load a CA profile group, and apply an SSL proxy profile to a security policy for logical systems.

[See [SSL Forward Proxy Overview](#).]

- Starting in Junos OS Release 19.1R1, the following features that are supported on the logical systems are now extended to tenant systems:
 - **Logging support for tenant systems (SRX1500, SRX4100, SRX4200, and SRX4600)**—Starting in Junos OS Release 19.1R1, on-box reporting configurations are supported for each tenant system, and logs are handled based on these configurations. Use the **set security log report** and **set security log mode stream** commands to enable the on-box reporting. The on-box reporting feature with stream mode is also supported on tenant systems.

[See [Security Log for Tenant Systems](#).]

- **User firewall enhanced support for tenant systems (SRX Series)**—Starting in Junos OS Release 19.1R1, support for user firewall authentication is enhanced using a shared model. In this model, tenant systems share user firewall configuration and authentication entries with the master logical system. The tenant system shares the authentication data collected from the local authentication, Active Directory authentication, firewall authentication, Juniper Identity Management Service (JIMS), and ClearPass authentication with the master logical system.

[See [Firewall Authentication for Tenant Systems](#).]

Routing Policy and Firewall Filters

- **Optional application configuration in a unified policy (SRX Series and vSRX)**—Starting in Junos OS Release 19.1R1, configuring the **application** statement at the **[edit security policies from-zone zone-name to-zone zone-name policy policy-name match]** hierarchy level is optional if the **dynamic-application** statement is configured at the same hierarchy level.

In releases before Junos OS Release 19.1R1, it is mandatory to configure the **application** statement even if the **dynamic-application** statement is configured.

[See [application \(Security Policies\)](#) and [dynamic-application \(Security Policies\)](#).]

Routing Protocols

- **Support for BGP graceful shutdown (SRX Series)**— Starting in Junos OS Release 19.1R1, graceful traffic migration from one BGP next hop to another is supported, without traffic interruption. Also, BGP administrative shutdown communication can be sent to the BGP peer.

You can configure both **graceful-shutdown** and **shutdown** statements at the **[edit protocols bgp]**, **[edit protocols bgp group group-name]**, and **[edit protocols bgp group group-name neighbor address]** hierarchy levels.

NOTE: Graceful shutdown is disabled by default.

[See: [graceful-shutdown \(Protocols BGP\)](#), [shutdown \(Protocols BGP\)](#).]

Security

- **Juniper Entropy Beacon (SRX Series)**—Starting in Junos OS Release 19.1R1, Juniper Entropy Beacon (JEB) allows authorized devices to request entropy packages from a SRX345 Services Gateway configured as a JEB server. Entropy is a crucial component of all cryptographic security systems because it is used to generate symmetric and asymmetric cryptographic keys. Low entropy leads to predictable keys, which can compromise the security of a system. JEB provides high quality entropy from a trusted source to entropy starved clients securely over the network.

[See [Juniper Entropy Beacon Overview](#)]

Unified Threat Management (UTM)

- **SRX TAP mode support for UTM features (SRX300, SRX320, SRX340, SRX345, SRX550HM, SRX1500, SRX4100, SRX4200, and SRX4600)**—Starting in Junos OS Release 19.1R1, the Unified Threat Management (UTM) module supports TAP (Terminal Access Point) mode. When you configure SRX Series device to operate in TAP mode, the device generates and displays security log information such as threats detected, application usage, and user details. When configured to operate in TAP mode, the SRX Series device receives packets only from the configured TAP interface.

[See [Enhanced Web Filtering](#).]

VPN

- **PowerMode IPsec with SPC3 (SRX5400, SRX5600, and SRX5800)**—Starting in Release 19.1R1, Junos OS on SRX Series devices with SPC3 supports a new mode of IPsec operation called PowerMode IPsec (PMI). PMI uses a small software block inside the Packet Forwarding Engine that bypasses flow processing and utilizes the Intel Advanced Encryption Standard New Instructions (AES-NI) for optimized performance of IPsec processing.

You can enable PMI processing by using the **power-mode-ipsec** statement at the **[edit security flow]** hierarchy level.

With PMI configured, the device supports the following features:

- Internet Key Exchange (IKE) functionality
- AutoVPN with traffic selectors
- High availability
- IPv6
- Stateful firewall
- st0 interface
- Traffic selectors

[See [Understanding PowerMode IPsec](#).]

- **Cryptographic algorithm support for IPsec and IKE on SRX5K-SPC3 card (SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 19.1R1, SRX5000 line of devices with SRX5K-SPC3 card support cryptographic algorithms to protect classified information.

The following algorithms are supported for IPsec:

- Diffie-Hellman Group 15
- Diffie-Hellman Group 16
- Diffie-Hellman Group 21
- HMAC-SHA-512
- HMAC-SHA-384

The following algorithms are supported for IKE:

- Diffie-Hellman Group 15
- Diffie-Hellman Group 16
- Diffie-Hellman Group 21
- SHA-512
- ECDSA-521 for X509 signatures

[See [IPsec VPN Overview](#) and [Understanding Certificates and PKI](#).]

- **Support for CoS classifier and rewrite functions in PMI on SPC3 (SRX Series)**— Starting in Junos OS Release 19.1R1, class of service (CoS) supports the configuration of behavior aggregate (BA) classifier, multifield (MF) classifier, and rewrite-rule functions in PowerMode IPsec (PMI) on SPC3 cards.

[See [Improving IPsec Performance with PowerMode IPsec](#).]

- **Support for IKE responder-only mode (SRX Series)**—Starting in Junos OS Release 19.1R1, two new options for the establishment of IPsec tunnels are introduced. The **responder-only** and **responder-only-no-rekey** options are added to the **establish-tunnels** statement under the **[edit security ipsec vpn vpn-name]** hierarchy level.

When you use these options, the VPN tunnel is established from the remote peer. In the case of the **responder-only** option, an established tunnel rekeys both Internet Key Exchange (IKE) and IPsec, based on the configured lifetime values. When you use the **responder-only-no-rekey** option, an established tunnel does not initiate rekeying from the device but relies on the remote peer to initiate rekeying.

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

SEE ALSO

Changes in Behavior and Syntax 229
Known Behavior 231
Known Issues 233
Resolved Issues 235
Documentation Updates 241
Migration, Upgrade, and Downgrade Instructions 242
Product Compatibility 243

Changes in Behavior and Syntax

IN THIS SECTION

- [Flow-Based and Packet-Based Processing | 230](#)
- [Network Management and Monitoring | 230](#)
- [Platform and Infrastructure | 230](#)
- [User Interface and Configuration | 230](#)
- [VPN | 230](#)

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 19.1R1 for the SRX Series.

Flow-Based and Packet-Based Processing

- **Change in the maximum number of sessions permitted(SRX340)**—Starting in Junos OS Release 19.1R1, SXR340 supports a maximum of 375,000 sessions permitted on a device configured without a license and a maximum of 256,000 sessions permitted on a device configured with a license.

In Junos OS releases before 19.1R1, SXR340 supported a maximum of 256,000 sessions permitted on a device configured without a license and a maximum of 128,000 sessions permitted on a device configured with a license.

[See [show security flow session](#)].

Network Management and Monitoring

- **NETCONF <kill-session> operation returns different values in <rpc-error> when the session identifier is equal to the current session ID (SRX Series)**—Starting in Junos OS Release 19.1R1, when you execute the <kill-session> NETCONF operation and the session identifier is equal to the current session ID, the values of the <error-type> and <error-tag> elements in the resulting <rpc-error> are **application** and **invalid-value**, respectively. In earlier releases, the <error-type> and <error-tag> values are **protocol** and **operation-failed**.

[See [<kill-session>](#).]

Platform and Infrastructure

- **Chassis cluster with SPC card (SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 19.1R1, when an SPC is acting as the CP (central point) as well as hosting the single control link port, this creates a single point of failure. If the SPC goes down on the primary node, the node is automatically rebooted to avoid a split-brain condition.

[See [Connecting SRX Series Devices to Create a Chassis Cluster](#)].

User Interface and Configuration

- **Options for monitor traffic interfaces statement added (SRX Series)**—Starting in Junos OS Release 19.1R1, the options **write-file** and **read-file** under the **monitor traffic** command are included in the visible CLI.

[See [monitor traffic](#).]

VPN

- **Certificate revocation list (SRX Series)**—Local certificates are being validated against certificate revocation list (CRL) even when CRL check is disabled. Starting in Junos OS Release 19.1R1, this can be stopped by disabling the CRL check through the Public Key Infrastructure (PKI) configuration. When CRL check is disabled, PKI will not validate local certificate against CRL.

[See [revocation-check \(Security PKI\)](#) and [Understanding Online Certificate Status Protocol and Certificate Revocation Lists](#).]

- **Encryption algorithm (SRX Series)**—Starting in Junos OS Release 19.1R1, when AES-GCM 128-bit or AES-GCM 256-bit encryption algorithms are configured in the IPsec proposal, it is not mandatory to configure AES-GCM encryption algorithm in the corresponding IKE proposal.

[See [IPsec VPN Configuration Overview](#) and [encryption-algorithm \(Security IKE\)](#).]

- **Local or remote certificates (SRX Series)**—Starting in Junos OS Release 19.1R1, a commit check is added to prevent user from adding ., /, %, and space in a certificate identifier while generating a local or remote certificates or a key pair.

[See [certificate-id \(Security\)](#) and [Example: Configuring PKI](#).]

- **Encryption algorithm support for high availability**—Starting in Junos OS Release 19.1R1, on SRX5000 line of devices, you can configure the **aes-128-cbc** option at **set security ipsec internal security-association manual encryption algorithm**. you configure this option for encrypting the high availability link.

[See [internal \(Security IPsec\)](#).]

SEE ALSO

[New and Changed Features | 217](#)

[Known Behavior | 231](#)

[Known Issues | 233](#)

[Resolved Issues | 235](#)

[Documentation Updates | 241](#)

[Migration, Upgrade, and Downgrade Instructions | 242](#)

[Product Compatibility | 243](#)

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 19.1R1 for the SRX Series.

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

Application Security

- SRX1500 with AppFW configured, the expected HTTP CPS is 60,000, which is a 14 percent drop (the expected value is 70,000). [PR1339131](#)

Flow-Based and Packet-Based Processing

- For J-Flow V9, only one collector can work under the families **inet** and **inet6** even RE CLI can be configured for 4 collectors under family **inet**. [PR1396482](#)

J-Web

- On SRX Series devices, the DHCP relay configuration under the Configure > Services > DHCP > DHCP Relay page is removed from J-Web in Junos OS Release 15.1X49-D60. The same DHCP relay can be configured using the CLI. [PR1205911](#)
- On SRX Series devices, DHCP Client Bindings under Monitor is removed. The same bindings can be seen in CLI using the **show dhcp client binding** command. [PR1205915](#)
- The CLI Terminal does not work in Java version 1.8 because of a security restriction in running the applet. [PR1341956](#)

Interfaces and Chassis

- When a USB device is under initialization, removing the USB device will lead to USB crash. [PR1332360](#)

Platform and Infrastructure

- The gRPC connection with the gRPC collector will reset upon RGO failover. [PR1402149](#)

SEE ALSO

[New and Changed Features | 217](#)

[Changes in Behavior and Syntax | 229](#)

[Known Issues | 233](#)

[Resolved Issues | 235](#)

[Documentation Updates | 241](#)[Migration, Upgrade, and Downgrade Instructions | 242](#)[Product Compatibility | 243](#)

Known Issues

IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 233](#)
- [Chassis Clustering | 233](#)
- [Flow-Based and Packet-Based Processing | 234](#)
- [J-Web | 234](#)
- [VPNs | 235](#)

This section lists the known issues in hardware and software in Junos OS Release 19.1R1 for SRX Series devices.

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

Application Layer Gateways (ALGs)

- On all SRX Series platforms, SIP/FTP ALG does not work when SIP traffic with source NAT goes through the SRX Series devices. [PR1398377](#)

Chassis Clustering

- On SRX Series devices with GPRS tunneling protocol version 2 (GTPv2) traffic logging configuration, the device might be potentially overwritten with an incorrect buffer address if the detailed logging is configured under the GTPv2 profile. As a result, it might reboot and cause an outage of the traffic. As a workaround, change the logging from detail to basic under the GTPv2 profile:

```
security gprs gtp profile gtp_profile {  
    timeout 3;  
    rate-limit 5000;
```

```

log {
    forwarded basic;
    state-invalid basic;
    prohibited basic;
    rate-limited {
        basic;
    }
}

```

[PR1413718](#)

Flow-Based and Packet-Based Processing

- On SRX1500 platforms, the system does not get reset by a watchdog when the CPU freezes. [PR1361843](#)
- On SRX1500 platform, the activity LED (right LED) for the 1-Gigabit Ethernet and 10-Gigabit Ethernet ports (xe-0/0/16 through xe-0/0/19) does not light up when the interface is up and passing traffic correctly. [PR1380928](#)
- With stress TCP traffic, some invalid sessions time out over 48 hours. [PR1383139](#)
- On all SRX Series platforms, in chassis cluster with Z mode traffic and local (non-reth) interfaces are configured, when using ECMP routing between multiple interfaces residing on both node0 and node1, if a session is initiated through one node and the return traffic comes in through the other node, packets may get dropped due to reroute failed. As a workaround, do not use ECMP between interfaces residing on different cluster nodes. Make sure that both directions of the flow sessions pass through the same cluster node. [PR1410233](#)
- Within an SSL-proxy configuration, if **trusted-ca** and **root-ca** have the same name, then it will result in the associated SSL-T and I profiles not getting pushed to the Packet Forwarding Engine and thereby impacting the SSL-proxy functionality. As a workaround, ensure to have different IDs or names for **trusted-ca** and **root-ca**.

If already in the scenario, do the following to recover:

- Configure different name for **trusted-ca** and **root-ca**.
- From CLI, restart NSD process using command **restart network-security**.

[PR1420859](#)

J-Web

- Forming an HA from J-Web by using the HA cluster wizard is not supported from Junos OS Release 12.1X47 onward for SRX5400 only. [PR1372518](#)

- On the SRX300 line of devices, an IPS installation failure message is displayed when uploading IPS signature package using the TAP mode quick setup wizard. This is an intermittent issue and occurs when IPS is installed immediately after the **system zeroized** command. As a workaround, retry to install the IPS package again. [PR1404296](#)

VPNs

- On SRX5400, SRX5600, and SRX5800 devices with SPC3, idle IPsec VPN tunnels without traffic and with ongoing DPD probes will be affected during the RGO failover window. The IPsec VPN process in the new primary Routing Engine may not be initialized on time to respond to the DPD probes. As a workaround, the user can increase the DPD interval to 20 seconds with the threshold set to 5 or make sure that there is traffic flowing through all the tunnels during the RGO failover window. [PR1405515](#)
- On SRX5400, SRX5600, and SRX5800 devices, during in-service software upgrade (ISSU), the IPsec tunnels flap causing a disruption of traffic. The IPsec tunnels recover automatically after the ISSU process is completed. [PR1416334](#)

SEE ALSO

[New and Changed Features | 217](#)

[Changes in Behavior and Syntax | 229](#)

[Known Behavior | 231](#)

[Resolved Issues | 235](#)

[Documentation Updates | 241](#)

[Migration, Upgrade, and Downgrade Instructions | 242](#)

[Product Compatibility | 243](#)

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 19.1R1 for SRX Series devices.

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

Application Security

- Fail to match permit rule in AppFW rule set. [PR1404161](#)

Application Layer Gateways (ALGs)

- DNS requests with the EDNS option might be dropped by the DNS ALG. [PR1379433](#)
- The H.323 protocol voice packets might be dropped. [PR1400630](#)

Chassis Clustering

- Traffic loss occurs when the primary node is rebooting. [PR1372862](#)
- If using SRX Series chassis cluster and configuring four 100-Gigabit Ethernet interfaces on PIC 0, all the four interfaces might be down. [PR1387701](#)
- Traffic cannot pass through cross tenants after ISSU from Junos OS Release 18.3 to Junos OS Release 18.4. [PR1382467](#)
- The flowd process might stop if doing an ISSU upgrade. [PR1386522](#)
- The VDSL is not stable if there are sudden noises after configuring VDSL SOS feature. [PR1387133](#)
- ISSU status with error from Junos OS Release 18.2R1-S1 or Junos OS Release 18.2R1-S2 to Junos OS Release 18.2R1-S3. [PR1387947](#)
- The cluster IDs larger than 10 will cause FPCs to remain in offline on SRX4600 chassis cluster. [PR1390202](#)
- The MACsec on a physical port might not initialize properly when a new node is joined to the chassis cluster. [PR1396020](#)
- The flowd process stops if updating or deleting a GTP tunnel. [PR1404317](#)

Flow-Based and Packet-Based Processing

- AppID classification logic has been improved for NetBIOS and RPC. [PR1357093](#)
- Control traffic loss may be seen on SRX4600 platform. [PR1357591](#)
- The Application identification (AppID) is supported for HTTP, SMTPS, POP3S, and IMAPS protocols. [PR1365810](#)
- When activating security flow traceoptions, the unfiltered traffic is captured. [PR1367124](#)
- Support for intelligent CLI-based autocomplete is added to secure-wire. [PR1372825](#)
- The pkid process might stop after RGO failover. [PR1379348](#)
- The reth interface flaps after doing an ISSU update. [PR1381475](#)

- Large file downloads slow down for many seconds. [PR1386122](#)
- Traffic might be processed by the VRRP backup when multiple VRRP groups are configured. [PR1386292](#)
- Traffic might be stopped after session created on SRX4600 platform. [PR1388735](#)
- The SRX Series device does not send messages frag needed and DF set back to the source host during path MTU discovery. [PR1389428](#)
- Packet loss might occur on unrelated traffic when AppQoS rate-limiter is applied on SRX4600 and SRX5000 platform using SPC3. [PR1394085](#)
- Request to display **dropped-illegal-packet** and **dropped-icmp-packet** configuration options. [PR1394720](#)
- Switching interface mode between family **ethernet-switching** and family **inet/inet6** might cause traffic loss. [PR1394850](#)
- These messages are seen: /kernel: tcp_timer_keep:Local(0x80000004:54652) Foreign(0x80000004:33160). [PR1396584](#)
- SRX Series devices connection to JIMS keeps flapping causes fail over to secondary JIMS. [PR1398140](#)
- On SRX4600 and SRX5000 devices, BGP packets might be dropped under high CPU usage. [PR1398407](#)
- VLAN push might not work on SRX1500. [PR1398877](#)
- Increase DAG feed scale number to 256 from 63. [PR1399314](#)
- The authd process might crash when issuing **show network-access requests pending** command during the authd restarting. [PR1401249](#)
- Unable to access to SRX Series platforms if the messages **kern.maxfiles limit exceeded by uid 65,534, please see tuning(7)** are seen. [PR1402242](#)
- Downloads may stall and/or completely fail when utilizing services that are reliant on TCP proxy. [PR1403412](#)
- Transit UDP 500/4500 traffic might not pass across SRX5000 Series devices when using SPC3/SPC2. [PR1403517](#)
- ISSU failed from Junos OS Release 18.3R1.9 to Junos OS Release 18.4R1.4. [PR1405556](#)
- The flowd process crashes and all cards are brought off. [PR1406210](#)
- The RG1 failover does not happen immediately when the SPC3 card crashes. [PR1407064](#)
- Session capacity of SRX340 is not match SRX345. [PR1410801](#)

Integrated User Firewall

- Future group membership updates are not recognized by IUFW after a user's sAMAccountName is changed while the distinguished name (DN) remained the same. [PR1394049](#)

Interfaces and Routing

- IPv4 multicast packets might not be broadcasted from the IRB interface on SRX1500 device. [PR1385934](#)
- SRX4600 10-gigabit Interface optics diagnostic access issue. [PR1395806](#)
- The 40-Gigabit and 100-Gigabit Ethernet ports may take a long time (about 30 s) to link up on SRX4600 platform. [PR1397210](#)
- High jsd or na-grpcd CPU usage might be seen when JET or JTI is not used. [PR1398398](#)
- SRX Series device cannot obtain IPv6 address through DHCPv6 when using a PPPoE interface with logical unit number greater than 0. [PR1402066](#)

Intrusion Detection and Prevention (IDP)

- Unable to deploy IDP due to the IDP configuration cannot be committed. [PR1374079](#)
- Performance drops are seen in SRX345 and SRX340 platforms for IDP C2S policy. [PR1395592](#)

Installation and Upgrade

- Junos OS Release 18.3R1 cannot be installed using TFTP in boot loader on SRX300 platforms. [PR1390858](#)

J-Web

- On SRX Series platforms, the root password configured at first J-Web access (Skip to J-Web) does not work if password length is shorter than eight characters. [PR1371353](#)
- In the J-Web dashboard, the Security Resources widget did not display absolute values. This is now corrected. [PR1372826](#)
- Excluded addresses within J-Web Security Policy editor were not sufficiently differentiated versus normal addresses. They are now highlighted red for ease of identification. [PR1376112](#)
- The next-hop IP address is not displayed in the routing table in the J-Web. [PR1398650](#)
- J-Web page do not load after login with logical-system specific user. [PR1396879](#)
- Special character used in the preshared key is removed silently after a commit operation on J-Web. [PR1399363](#)

- Configuring using the CLI Editor in the J-Web generates an mgd core file. [PR1404946](#)
- The httpd-gk process crashes, leading to dynamic VPN failures and high Routing Engine CPU utilization 100 percent. [PR1414642](#)

Layer 2 Ethernet Services

- DHCPv6 clients might fail to get addresses on SRX Series platforms. [PR1392723](#)

Multiprotocol Label Switching (MPLS)

- BGP and OSPF flapped to cause traffic loss with RPD core on SRX550M cluster. [PR1366575](#)

Network Address Translation (NAT)

- The SRX Series devices might send the **noSuchInstance** value to the SNMP server in get-response during commit. [PR1357840](#)
- NAT64 and traceroute do not work correctly on an SRX Series device. [PR1376890](#)
- SPC3 mix mode NAT core at `../sysdeps/unix/sysv/linux/raise.c:55`. [PR1403583](#)

Platform and Infrastructure

- High httpd utilization after reboot failover. [PR1352133](#)
- Many chassis commands missing. [PR1363645](#)
- IP monitoring failure resulting in multiple interfaces disappearing from forwarding table. [PR1371500](#)
- Some error messages could be seen when running **show interface extensive** command from CLI or Junos Space. [PR1380439](#)
- Traffic loss seen in Layer 2 VPN with GRE tunnel. [PR1381740](#)
- Redundancy group failover caused by interface monitoring failure is slow to master state at PFE. [PR1385521](#)
- Login class with allowed-days and specific access-start/access-end does not work as expected. [PR1389633](#)
- GW lcores and srpxfe cores at `../src/pfe/usp/rt/applications/ipsec/ipsec_rt_forge_util.c:59` when loading 18.4 image. [PR1392580](#)
- The flowd process crashes if it goes into a dead loop. [PR1403276](#)
- HA failed with the failure code **HW** after loading the image. [PR1406029](#)

Routing Policy and Firewall Filters

- When SSL-Forward-Poxy is configured in a unified policy along with the action of Reject+Redirect, a block page was not presented to the user for HTTPS sites. [PR1375823](#)
- The **show security flow session** command now fully supports the dynamic-application construct. [PR1387449](#)
- The nsd process crashes and generates a core file. [PR1388719](#)

Routing Protocols

- vFPC may continuously crash on vMX platform. [PR1364624](#)

Services Applications

- SRX5600 HA SPC2, the ICAP redirect objects are in use even after clearing TCP sessions. [PR1390835](#)

Software Installation and Upgrade

- Fan speed goes up and down continuously on SRX1500. [PR1335523](#)

Unified Threat Management (UTM)

- Source and destination zone information are added in the UTM log. [PR1326271](#)
- EWF server status shows UP when 443 is specified as server port. [PR1383695](#)
- Whitelist/Blacklist does not work for HTTPS traffic going through the Web proxy. [PR1401996](#)
- On SRX Series, when configuring Enhanced Web Filtering on the CLI, the autocomplete function did not properly handle or suggest custom categories. [PR1406512](#)
- On SRX Series, when using Unified Policies and Webfiltering (EWF) without SSL-Proxy in Junos OS Release 18.4R1, the Server Name Indication (SNI) may not be identified correctly and the RT_UTM logs were recording incomplete information. [PR1410981](#)

VPNs

- ISSU from Junos OS.Release 15.1X49-D120 to Junos OS.Release 15.1X49-D130 seeing KMD core seen at **0x08228b83** in `iked_advpn_timer_cb_delete_inactive_shortcut_tunnel` (`timer_ctx=0x99d8000`) at `../..../src/usp/usr.sbin/iked/core/iked_advpn.c:227`. [PR1340973](#)
- Dot usage in CA profile name causes issues when the pkid process is restarted. [PR1351727](#)

- A few VPN tunnels do not forward traffic after RG1 failover. [PR1394427](#)
- The kmd process might crash when SNMP polls for the IKE SA. [PR1397897](#)
- VPN does not recover on the high-end standalone SRX Series device when CLI operation **restart ipsec-key-management** is done. [PR1400712](#)
- Syslog is not generated when the ike gateway rejects a duplicate IKE ID connection. [PR1404985](#)
- Not all the tunnels are deleted when the authentication algorithm in IPsec proposal is changed. [PR1406020](#)
- Multiple flowd core files are observed with IPsec acceleration with fragmentation traffic. [PR1407910](#)
- Traffic drops on peer due to bad SPI after first re-authentication. [PR1412316](#)

SEE ALSO

[New and Changed Features | 217](#)

[Changes in Behavior and Syntax | 229](#)

[Known Behavior | 231](#)

[Known Issues | 233](#)

[Documentation Updates | 241](#)

[Migration, Upgrade, and Downgrade Instructions | 242](#)

[Product Compatibility | 243](#)

Documentation Updates

There are no errata or changes in Junos OS Release 19.1R1 documentation for the SRX Series.

SEE ALSO

[New and Changed Features | 217](#)

[Changes in Behavior and Syntax | 229](#)

[Known Behavior | 231](#)

[Known Issues | 233](#)

[Resolved Issues | 235](#)

[Migration, Upgrade, and Downgrade Instructions | 242](#)

[Product Compatibility | 243](#)

Migration, Upgrade, and Downgrade Instructions

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

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

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 15.1X49, 17.3, 17.4, 18.1, and 18.2 are EEOL releases. You can upgrade from one Junos OS Release to the next release or one release after the next release. For example you can upgrade from Junos OS Release 15.1X49 to Release 17.3 or 17.4, Junos OS Release 17.4 to Release 18.1 or 18.2, and from Junos OS Release 18.1 to Release 18.2 or 18.3 and so on.

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

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

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

For information about ISSU, see the [Chassis Cluster User Guide for Security Devices](#).

SEE ALSO

[New and Changed Features | 217](#)

[Changes in Behavior and Syntax | 229](#)

[Known Behavior | 231](#)

[Known Issues | 233](#)

[Resolved Issues | 235](#)

[Documentation Updates | 241](#)

[Product Compatibility | 243](#)

Product Compatibility

Hardware Compatibility

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

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

SEE ALSO

[New and Changed Features | 217](#)

[Changes in Behavior and Syntax | 229](#)

[Known Behavior | 231](#)

[Known Issues | 233](#)

[Resolved Issues | 235](#)

[Documentation Updates | 241](#)

[Migration, Upgrade, and Downgrade Instructions | 242](#)

Upgrading Using ISSU

In-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic.

For additional information about using ISSU on routing and switching devices, see the [High Availability User Guide](#).

For additional information about using ISSU on security devices, see the [Chassis Cluster User Guide for SRX Series Devices](#).

For information about ISSU support across platforms and Junos OS releases, see the [In-Service Software Upgrade \(ISSU\)](#) Web application.

Licensing

Starting in 2019, Juniper Networks introduced a new software licensing model. The Juniper Flex Program is a framework, set of policies, and tools that help unify and thereby simplify the multiple product-driven licensing and packaging approaches that have been developed at Juniper Networks over the past several years.

The major components of the framework are:

- A focus on customer segments (enterprise, service provider, and cloud) and use cases for Juniper Networks hardware and software products.
- The introduction of a common three-tiered model (standard, advanced, and premium) for all Juniper Networks software products.
- The introduction of subscription licenses and subscription portability for all Juniper Networks products, including Junos OS and Contrail.

For information on the list of supported products, see [Juniper Flex Program](#).

Compliance Advisor

For regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

Finding More Information

For the latest, most complete information about known and resolved issues with the Junos OS, see the Juniper Networks Problem Report Search application at <https://prsearch.juniper.net>.

For regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

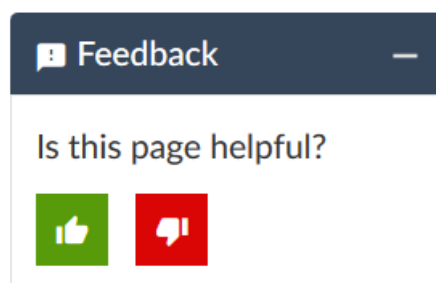
To access Software Release Notifications for Junos OS Service Releases, visit our Knowledge Center at <https://support.juniper.net/support/>. You'll need to log in to your Juniper Account. From the Knowledge Center, search by the specific release number, for example 17.4R1-S2. Use the Software Release Notifications to download software, and learn about known and resolved issues for specific service releases.

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://apps.juniper.net/feature-explorer/>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://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/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

Revision History

25 November 2021—Revision 20, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

15 July 2021—Revision 19, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

6 December 2019—Revision 18, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

31 October 2019—Revision 17, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

10 October 2019—Revision 16, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

26 September 2019—Revision 15, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

23 July 2019—Revision 14, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

18 July 2019—Revision 13, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

4 July 2019—Revision 12, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

27 June 2019—Revision 11, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

20 June 2019—Revision 10, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

6 June 2019—Revision 9, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

28 May 2019—Revision 8, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

9 May 2019—Revision 7, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

2 May 2019—Revision 6, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

19 April 2019—Revision 5, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

11 April 2019—Revision 4, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

9 April 2019—Revision 3, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

3 April 2019—Revision 2, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

27 March 2019—Revision 1, Junos OS Release 19.1R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.