Release Notes

Published
2023-11-24

Junos® OS Release 21.4R2

Table of Contents

Introduction | 1

Junos OS Release Notes for ACX Series

What's New | 2

What's New in 21.4R2 | **2**

What's New in 21.4R1 | **2**

Routing Protocols | **2**

Software Installation and Upgrade | **3**

Additional Features | **4**

What's Changed | 4

What's Changed in Release 21.4R2 | **5**

What's Changed in Release 21.4R1 | **5**

Known Limitations | 6

Open Issues | 7

Resolved Issues | 9

Resolved Issues: 21.4R2 | **9**

Resolved Issues: 21.4R1 | **11**

Documentation Updates | 13

Migration, Upgrade, and Downgrade Instructions | 13

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | **13**

Junos OS Release Notes for cSRX

What's New | 15

What's Changed | 15

Known Limitations | 15

Open Issues | 15

Resolved Issues | 16

Documentation Updates | 16

Junos OS Release Notes for EX Series

What's New | 17

What's New in 21.4R2 | **17**

What's New in 21.4R1 | **17**

EVPN | **17**

High Availability | **18**

Additional Features | **19**

What's Changed | 20

What's Changed in Release 21.4R2 | **20**

What's Changed in Release 21.4R1 | **21**

Known Limitations | 22

Open Issues | 23

Resolved Issues | 27

Resolved Issues: 21.4R2 | **27**

Resolved Issues: 21.4R1 | **30**

Documentation Updates | 36

Migration, Upgrade, and Downgrade Instructions | 36

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | **37**

Junos OS Release Notes for JRR Series

What's New | 38

What's Changed | 38

Known Limitations | 39

Open Issues | 39

Resolved Issues | 39

Resolved Issues: 21.4R2 | 39

Resolved Issues: 21.4R1 | 40

Documentation Updates | 40

Migration, Upgrade, and Downgrade Instructions | 40

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 41

Junos OS Release Notes for Juniper Secure Connect

What's New | 42

What's New in 21.4R2 | 42

What's New in 21.4R1 | 43

Authentication and Access Control | 43

What's Changed | 43

Known Limitations | 43

Open Issues | 44

Resolved Issues | 44

Documentation Updates | 44

Junos OS Release Notes for Junos Fusion for Enterprise

What's New | 45

What's Changed | 45

Known Limitations | 45

Open Issues | 45

Resolved Issues | 46

Documentation Updates | 46

Migration, Upgrade, and Downgrade Instructions | 46

Junos OS Release Notes for Junos Fusion for Provider Edge

What's New | 52

What's Changed | 53

Known Limitations | 53

Open Issues | 53

Resolved Issues | 53

Documentation Updates | 53

Migration, Upgrade, and Downgrade Instructions | 54

Junos OS Release Notes for MX Series

What's New | 64

What's New in 21.4R2 | **64**

What's New in 21.4R1 | **64**

Hardware | **65**

Architecture | **74**

Chassis | **75**

EVPN | **75**

High Availability | **76**

IP Tunneling | **76**

Junos Telemetry Interface (JTI) | **76**

Layer 2 VPN | **76**

Interfaces | **77**

MPLS | **77**

Multicast | **77**

Network Address Translation (NAT) | **77**

Operation, Administration, and Maintenance (OAM) | **78**

Platform and Infrastructure | **78**

Routing Protocols | **79**

Source Packet Routing in Networking (SPRING) or Segment Routing | **79**

Services Applications | **80**

Software Defined Networking (SDN) | **80**

Software Installation and Upgrade | **80**

Subscriber Management and Services | **82**

VPNs | **83**

Additional Features | **84**

What's Changed | 86

What's Changed in Release 21.4R2 | **86**

What's Changed in Release 21.4R1 | **88**

Known Limitations | 90

Open Issues | 94

Resolved Issues | 107

Resolved Issues: 21.4R2 | **107**

Resolved Issues: 21.4R1 | **120**

Documentation Updates | 138

Migration, Upgrade, and Downgrade Instructions | 138

Junos OS Release Notes for NFX Series

What's New | 145

What's New in 21.4R2 | **145**

Virtualized Network Functions (VNFs) | **145**

What's New in 21.4R1 | **145**

Network Management and Monitoring | **146**

What's Changed | 146

Known Limitations | 146

Open Issues | 146

Resolved Issues | 148

Resolved Issues: 21.4R2 | **148**

Resolved Issues: 21.4R1 | **149**

Documentation Updates | 150

Migration, Upgrade, and Downgrade Instructions | 150

Junos OS Release Notes for PTX Series

What's New | 152

What's New in 21.4R2 | **153**

What's New in 21.4R1 | **153**

Hardware | **153**

Class of Service | **153**

MPLS | **154**

Routing Protocols | **154**

Services Applications | **155**

Software Installation and Upgrade | **155**

Additional Features | **157**

What's Changed | 157

What's Changed in Release 21.4R2 | **157**

What's Changed in Release 21.4R1 | **159**

Known Limitations | 161

Open Issues | 161

Resolved Issues | 163

Resolved Issues: 21.4R2 | **164**

Resolved Issues: 21.4R1 | **165**

Documentation Updates | 169

Migration, Upgrade, and Downgrade Instructions | 170

Junos OS Release Notes for QFX Series

What's New | 175

What's New in 21.4R2 | **175**

EVPN | **175**

What's New in 21.4R1 | **177**

EVPN | **178**

High Availability | **179**

Juniper Extension Toolkit (JET) | **180**

Junos Telemetry Interface (JTI) | **180**

Licensing | **180**

MPLS | **181**

Network Management and Monitoring | 181
Operation, Administration, and Maintenance (OAM) | 182
Routing Policy and Firewall Filters | 182
Routing Protocols | 183
Services Applications | 184
Additional Features | 185

What's Changed | 186

What's Changed in Release 21.4R2 | 186
What's Changed in Release 21.4R1 | 187

Known Limitations | 188

Open Issues | 190

Resolved Issues | 194

Resolved Issues: 21.4R2 | 194
Resolved Issues: 21.4R1 | 199

Documentation Updates | 204

Migration, Upgrade, and Downgrade Instructions | 205

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 217

Junos OS Release Notes for SRX Series

What's New | 219

What's New in 21.4R2 | 219
What's New in 21.4R1 | 219
Application Identification (AppID) | 220
Authentication and Access Control | 220
Chassis | 220
Chassis Cluster-specific | 221
Flow-Based and Packet-Based Processing | 221
Hardware | 221
J-Web | 222
Network Address Translation (NAT) | 223
Platform and Infrastructure | 223

Software Installation and Upgrade | 224

Unified Threat Management (UTM) | 224

Additional Features | 225

What's Changed | 225

What's Changed in Release 21.4R2 | 226

What's Changed in Release 21.4R1 | 227

Known Limitations | 230

Open Issues | 231

Resolved Issues | 233

Resolved Issues: 21.4R2 | 233

Resolved Issues: 21.4R1 | 238

Documentation Updates | 244

Migration, Upgrade, and Downgrade Instructions | 244

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 244

Junos OS Release Notes for vMX

What's New | 246

What's New in 21.4R2 | 246

What's New in 21.4R1 | 246

Licensing | 246

Operation, Administration, and Maintenance (OAM) | 247

What's Changed | 247

What's Changed in Release 21.4R2 | 248

What's Changed in Release 21.4R1 | 248

Known Limitations | 249

Open Issues | 249

Resolved Issues | 250

Resolved Issues: 21.4R2 | 250

Resolved Issues: 21.4R1 | 250

Documentation Updates | 251

Upgrade Instructions | 251

Junos OS Release Notes for vRR

What's New | 252

What's Changed | 252

Known Limitations | 252

Open Issues | 252

Resolved Issues | 253

Resolved Issues: 21.4R2 | 253

Resolved Issues: 21.4R1 | 253

Documentation Updates | 254

Junos OS Release Notes for vSRX

What's New | 254

What's New in 21.4R2 | 255

What's New in 21.4R1 | 255

Application Identification (AppID) | 255

Authentication and Access Control | 255

Flow-Based and Packet-Based Processing | 256

Interfaces | 256

Licensing | 256

Platform and Infrastructure | 257

Unified Threat Management (UTM) | 257

Additional Features | 258

What's Changed | 258

What's Changed in Release 21.4R2 | 259

What's Changed in Release 21.4R1 | 260

Known Limitations | 261

Open Issues | 261

Resolved Issues | 262

Resolved Issues: 21.4R2 | **263**

Resolved Issues: 21.4R1 | **264**

Documentation Updates | 266

Migration, Upgrade, and Downgrade Instructions | 267

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | **273**

Licensing | 274

Finding More Information | 275

Requesting Technical Support | 275

Revision History | 277

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion Enterprise, Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

These release notes accompany Junos OS Release 21.4R2 for the ACX Series, Containerized Routing Protocol Process (cRPD), cSRX Container Firewall (cSRX), EX Series, JRR Series, Juniper Secure Connect, Junos Fusion Enterprise,Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, virtual MX Series router (vMX), Virtual Route Reflector (vRR), and vSRX Virtual Firewall (vSRX). They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Junos OS Release Notes for ACX Series

IN THIS SECTION

- What's New | 2
- What's Changed | 4
- Known Limitations | 6
- Open Issues | 7
- Resolved Issues | 9
- Documentation Updates | 13
- Migration, Upgrade, and Downgrade Instructions | 13

These release notes accompany Junos OS Release 21.4R2 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

- What's New in 21.4R2 | 2
- What's New in 21.4R1 | 2

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

What's New in 21.4R2

There are no new features or enhancements to existing features in Junos OS Release 21.4R2 for the ACX Series.

What's New in 21.4R1

IN THIS SECTION

- Routing Protocols | 2
- Software Installation and Upgrade | 3
- Additional Features | 4

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

Routing Protocols

- **OSPF link delay measurement and advertising (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.4R1, you can measure and advertise various performance metrics in IP networks with scalability through probe messages that are sent by Two-Way Active Measurement Protocol (TWAMP) Light. OSPF receives probe messages and the measured values from TWAMP Light. OSPF advertises these messages as TLVs in packets. You can use these metrics to make path-selection decisions based on the network performance.

  [See How to Enable Link Delay Measurement and Advertising in OSPF.]

- **Support for FAD and FAPM on traffic engineering database and BGP-LS (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.4R1, we support FlexAlgo Definition (FAD) and FlexAlgo Prefix Metric (FAPM) on the traffic engineering database and BGP Link State (BGP-LS). You can store FAD and FAPM entries in the traffic engineering database and BGP-LS. You can also store multiple prefix segment identifiers (SIDs) for a prefix in BGP-LS. You can import the FAD and FAPM entries from the traffic engineering database to BGP-LS and export the FAD entries from BGP-LS to the traffic engineering database.

  [See What is Flexible Algorithm Definition (FAD).]

Software Installation and Upgrade

- **Migration of Linux kernel version**—Starting in Junos OS Release 21.4R1, the following devices support the Wind River LTS19 kernel version:

Platforms	Routing Engine Supported
ACX5448, ACX5448-D, and ACX5448-M	RE-ACX-5448
MX240, MX480, and MX960	RE-S-X6
MX2020 and MX2010	REMX2K-X8
MX204	RE-S-1600x8
MX10003	RE-S-1600x8
MX2008	REMX2008-X8
MX10008, and MX10016	RE X10
PTX1000	RE-PTX1000
PTX5000	RE-PTX-X8
PTX10002	RE-PTX10002-60C
PTX10008	RE-PTX-2X00x4/RE X10
PTX10016	RE-PTX-2X00x4/RE X10

(Continued)

Platforms	Routing Engine Supported
QFX10002	RE-QFX10002-60C
EX9204, EX9208, and EX9214	EX9200-RE2
EX9251	EX9251-RE
EX9253	EX9253-RE
SRX5400, SRX5600, and SRX5800	SRX5K-RE3 (SRX5k RE-2000x6)

Starting in Junos OS Release 21.4R1, in order to install VM Host image based on Linux WR LTS19, you have to upgrade the i40e NVM firmware to version 7.0 or later.

[See Upgrading the i40e NVM Firmware on Routing Engines with VM Host Support .]

Additional Features

We've extended support for the following features to these platforms.

- **G.8275.1 Telecom profile support** (ACX5448)
  [See G.8275.1 Telecom profile support.]
- **Supported transceivers, optical interfaces, and DAC cables** (ACX Series, EX Series, PTX Series, MX Series, and QFX Series).—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

- What's Changed in Release 21.4R2 | 5
- What's Changed in Release 21.4R1 | 5

Learn about what changed in this release for ACX Series routers.

What's Changed in Release 21.4R2

IN THIS SECTION

- Network Management and Monitoring | 5

Network Management and Monitoring

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

What's Changed in Release 21.4R1

IN THIS SECTION

- EVPN | 6
- Network Management and Monitoring | 6

EVPN

- **Output for the show Ethernet switching flood extensive command**—The output for the `show ethernet-switching flood extensive` command now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as unilist. Previously, the output for the `show ethernet-switching flood extensive` command would misidentify the next-hop type as composite.

Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.

Known Limitations

IN THIS SECTION

- General Routing | 6

Learn about known limitations in Junos OS Release 21.4R2 for ACX Series routers.

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

General Routing

- The "ping" command on an ACX device might show variable latency values. This is expected for host-generated ICMP traffic due to the design of the PFE queue polling the packets from ASIC. PR1380145
- ACX: "Host 0 PCI Device not responding 0x14e4:0x9800" alarm is seen with LTS19 image upgrade. PR1602746

- Inline BFD session will not detect change in the remote multiplier when it is changed on-fly. PR1631910

Open Issues

IN THIS SECTION

- General Routing | 7
- Routing Protocols | 8
- VPNs | 8

Learn about open issues in Junos OS Release 21.4R2 for ACX Series routers.

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

General Routing

- For ACX710, if the console cable is plugged in and the terminal connection is active and sending characters to the interface, the system boot might be interrupted and the ACX710 boot will be stalled at the uboot# prompt. PR1513553
- Due to BRCM KBP issue route lookup might fail. Need to upgrade KBP to address this issue, Due to high risk KBP SDK upgrade planned for 21.1. PR1533513
- On ACX5448 platforms, if hierarchical-scheduler is configured for an interface, during interface flaps or configuration changes, some of Packet Forwarding Engine buffers might become out of sync, which might cause packet drops even without congestion. PR1603622
- On ACX platforms, traffic issue might be observed with downstream devices when Precision Time Protocol (PTP) is configured (G.8275.1 PTP profile) along with PHY timestamping and Multiprotocol Label Switching (MPLS) terminated on 10G interface. The transit PTP IPv4 packets are updated with incorrect Correction Factor(CF). This issue could be restored by disabling PHY stamping. However, disabling might impact the PTP performance. PR1612429

- For ACX5448, MX204, and MX2008 "VM Host-based" platforms, starting with Junos OS Release 21.4R1 or later, ssh and root login is required for copying line card image (chspmb.elf for MX2008) from Junos VM to Linux host during installation. The ssh and root login are required during installation. Use "deny-password" instead of "deny" as default root-login option under ssh config to allow internal trusted communication. Ref https://kb.juniper.net/TSB18224. PR1629943
- When multihop BFD is configured in ACX5448, delegated BFD sessions are not coming up. PR1633395
- When ACX710/5448 series platforms work as provider edge nodes in Layer 3 VPN environment, it might stop forwarding Layer 3 VPN traffic after core-facing link flaps, due to a race condition that happens during Layer 3 VPN NH programming in Packet Forwarding Engine. PR1635801
- Delegated/Inline BFD sessions configured in non-default VR will not work as support for L3 Inject is missing. PR1649806
- On ACX5448 and ACX710 platforms, traffic drop might be observed for some MAC entries which are learned on interchassis control link (ICL) instead of multichassis link aggregation (MC-AE). PR1653926

Routing Protocols

- When inline add event for IPv6 inline BFD session comes without resolving neighbor for nexthop , inline event addition will fail. PR1650677

VPNs

- On all Junos platforms with MVPN scenario, stale PIM (S, G) state might be seen when there are no local/remote receivers and the multicast source is inactive. Only stale PIM entry will be seen, and it doesn't impact MVPN service or functionalities. PR1536903

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.4R2 | 9
- Resolved Issues: 21.4R1 | 11

Learn about the issues fixed in this release for ACX Series routers.

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

Resolved Issues: 21.4R2

IN THIS SECTION

- General Routing | 9
- Platform and Infrastructure | 10
- Routing Protocols | 11

General Routing

- ACX710 running Junos OS Release 21.2R1 onwards might experience kernel crash. PR1608852
- Traffic might be dropped on ACX5448 and ACX710. PR1612026
- ACX5448: CFMD core files might be seen if CCM configuration is changed from ae ifl to physical ifl, and if the physical ifl was previously part of ae bundle. PR1612212
- In ACX5448, at rates above 4GB, there might be mismatches in statistics between the physical and logical interfaces. PR1614550
- Traffic might not be forwarded after failover in L2circuit hot standby mode. PR1616892
- On ACX5448 and ACX710 platforms with Layer 3 VPN scenarios after multiple core link or protocol flaps, the errors might be observed. PR1621425

- ACX5448 CoS - EXP rewrite is not working in layer 3 VPN scenario when mf filter is configured. PR1623922
- On ACX5000 Local fault and Remote fault signaling is not logged on **/var/log/messages**. PR1624761
- Unicast packet loss might be observed due to control-word configuration. PR1626058
- VPLS traffic loss might be observed post route flap. PR1626267
- PFE might crash after device reboot or PFE restart. PR1626503
- ACX2000: Output packet statistics are not incremented on the unit even after configuring statistics. PR1627040
- Multicast traffic drop might be seen if IGMP snooping is enabled for VLAN. PR1628600
- ACX5048 filters reporting TCAM errors are not installed in hardware after the upgrade from Junos OS Release 17.4R2-S8 to Release 20.4R3. PR1630280
- ACX710 running G.8275.2 stuck at PTP Acquiring state if the connection is through some timing unaware nodes. PR1632761
- Speed 10m configuration error on ACX5048 and ACX5096 platforms. PR1633226
- The storm-control rate-limit might not work with VPLS policer under IFL. PR1633427
- DHCP clients might not come online for IRB+VLAN/EVPN scenario. PR1633778
- IS-IS last transition time never increments. PR1634747
- IPv6 BFD session over AE interface might remain down on ACX5448/ACX710 platforms. PR1635020
- The LACP delay might be observed with an "aggregate wait time" of more than 1 second. PR1635763
- ACX5448 PEM overload alarm threshold is incorrect. PR1636222
- Locally switched traffic might be dropped on ACX5448 with ESI configured. PR1638386
- Layer 3 interface creation might fail on the ACX5448 and ACX710 platforms. PR1638581
- High priority packets might be dropped on ACX5448 platform. PR1642187

Platform and Infrastructure

- vmxt_lnx core file is found @ topo_get_link jnh_features_get_jnh jnh_stream_attach. PR1638166

Routing Protocols

- For prefixes leaked from BGP to IS-IS, the P flag will be set for Prefix-SID advertised from IS-IS. PR1627322

Resolved Issues: 21.4R1

IN THIS SECTION

- General Routing | 11

General Routing

- On ACX5448 routers, the BFD session status goes in the `Init` state after the system reboots when you have both CFM and BFD configured on the system. PR1552235
- Packet buffer allocation failed messages might be generated when you use the scaled-CFM sessions with minimum DM or SLM cycle-time along with enhanced-sla-iterator. PR1574754
- On ACX5448 routers, the asynchronous-notification for 1G interface fails. PR1580700
- On ACX5448 routers, IPv4 traffic loss with packet size more than 1410 occurs. PR1584509
- On ACX710 routers, PTP might get stuck and not function properly in a certain condition. PR1587990
- On ACX710 and ACX5400 routers, traffic might get forwarded through the member links in the `Down` state after the new member links gets added to the aggregated Ethernet interface. PR1589168
- On ACX5448 routers, high DMR out of sequence with iterator configuration occurs. PR1596050
- On ACX710 routers, the l2ald process generates core file at `l2ald_event_process_list_id`, `l2ald_event_proc_all_lists`, and `l2ald_event_periodic ()` at **../../../../../../src/junos/usr.sbin/l2ald/l2ald_event.c:757**. PR1596908
- On ACX5448 and ACX710 routers, traffic drop in the EVPN VPWS flexible cross connect occurs. PR1598074
- On ACX710 and ACX5448 routers, traffic loss might be observed if you modify drop-profiles. PR1598595
- On ACX710 routers, the rpf-check-bytes,rpf-check-packets counters does not get updated properly to the flat file as expected. PR1600513

- On ACX5448 and ACX710 routers, MACsec traffic over Layer 2 circuit might not work. PR1603534
- On ACX5448 routers, FPC might restart when you execute the `show firewall`. PR1605288
- The optics_mts_010.robot script fails while verifying SNMP and matching the CLI values. PR1605348
- On ACX5448 and ACX710 routers running DHCP, relay does not process packets arriving over MPLS. PR1605854
- On ACX1100 routers, the FEB (Forwarding Engine Board) might crash. PR1606424
- On ACX710 and ACX5448 routers, the DHCP packets might not be relayed. PR1608125
- On ACX5096 routers, the pps traffic output appears on the deactivated interfaces. PR1608827
- On ACX710 routers running Junos OS Release 21.2R1 and later might experience kernel crash. PR1608852
- The routing protocol engine CPU becomes nonresponsive at 100 percent. PR1612387
- Interface state gets reset after the Packet Forwarding Engine restarts. PR1613314
- On ACX5448 routers, unknown SMART attributes for StorFly VSFBM6CC100G-JUN1 SSD might occur. PR1614068
- On ACX5448 and ACX710 routers with Layer 3 VPN scenarios, error messages might be generated after multiple core link or protocol flaps. PR1621425
- On ACX5448 routers, CFM does not appear to be in the `Ok` state after the router reboots. PR1602489
- On ACX5448 and ACX710 routers, traffic towards the CE device through the default route might be dropped in VRF. PR1611651
- Traffic might get equally load-balanced irrespective of the scheduler configuration. PR1620137
- Six to eight seconds of delay occurs when the receiver switches in between groups. PR1620685
- Traffic does not get forwarded to one of the the single homed PE device after you change the VLAN-ID under the routing instance. PR1621036
- On ACX5448 routers, the smartd configurations do not get applied. PR1623359

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for ACX Series.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | **13**

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

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

NOTE: Starting in Junos OS Release 21.4R1 and later releases, `ssh root-login` is required for copying the line card image (chspmb.elf) from Junos OS VM to Linux host during installation for ACX5448 VM host based platforms. Do not disable it through configuration during installation. Use `deny-password` instead of `deny` as default root-login option under `ssh` configuration to allow internal trusted communication.

For information on VMHost based platforms, see VM Host Overview (Junos OS).

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

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

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

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

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

Table 1: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for cSRX

IN THIS SECTION

- What's New | 15
- What's Changed | 15
- Known Limitations | 15
- Open Issues | 15
- Resolved Issues | 16

- Documentation Updates | 16

These release notes accompany Junos OS Release 21.4R1 for the cSRX Container Firewall, a containerized version of the SRX Series Services Gateway. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features or enhancements to existing features in Junos OS Release 21.4R1, 21.4R2, and 21.4R3 for cSRX Container Firewall.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R1, 21.4R2, and 21.4R3 for cSRX Container Firewall.

Known Limitations

There are no known limitations in hardware and software in Junos OS 21.4R3 for cSRX Container Firewall.

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

Open Issues

There are no known issues in hardware and software in Junos OS Release 21.4R3 for cSRX Container Firewall.

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

Resolved Issues

There are no resolved issues in Junos OS Release 21.4R1, 21.4R2, and 21.4R3 for cSRX Container Firewall.

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

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for cSRX Container Firewall.

Junos OS Release Notes for EX Series

IN THIS SECTION

- What's New | 17
- What's Changed | 20
- Known Limitations | 22
- Open Issues | 23
- Resolved Issues | 27
- Documentation Updates | 36
- Migration, Upgrade, and Downgrade Instructions | 36

These release notes accompany Junos OS Release 21.4R2 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

- What's New in 21.4R2 | 17
- What's New in 21.4R1 | 17

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

What's New in 21.4R2

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

What's New in 21.4R1

IN THIS SECTION

- EVPN | 17
- High Availability | 18
- Additional Features | 19

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

EVPN

- **Support for EVPN-VXLAN group-based policies (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, and EX4650-48Y-VC)**—Starting in Junos OS Release 21.4R1, EX4400 and EX4650 switches provide standards-based multi-level segmentation (also called group-based policy, or GBP) on the basis of Layer 3 virtual networks and group-based tags rather than IP-based filters. GBP supports an application-centric policy model that

separates network access policies from the underlying network topology through the use of policy tags, thus allowing different levels of access control for endpoints and applications even within the same VLAN.

The EX4400 and EX4650 switches also provide GBP support for locally switched traffic on VXLAN access ports.

[See Micro and Macro Segmentation using Group Based Policy in a VXLAN.]

- **Dynamic overlay load balancing in an EVPN-VXLAN network (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T)** —Starting in Junos OS Release 21.4R1, EX4400 switches in an EVPN-VXLAN network (centrally routed and edge-routed bridging overlays) support dynamic load balancing on virtual tunnel endpoints (VTEPs). Juniper Networks switches have dynamic load balancing enabled by default.

  [See Dynamic Load Balancing in an EVPN-VXLAN Network.]

- **Interconnecting EVPN-VXLAN data centers with EVPN-MPLS in a WAN using gateway nodes (MX-Series, EX9200, EX9252, EX9253)**—Starting in Junos OS Release 21.4R1, you can interconnect EVPN-VXLAN data centers with EVPN-MPLS in a WAN using gateway nodes, but without using logical tunnel interfaces. In Release 21.4R1, you can interconnect only those BDs/VLANs that are on the interconnected VLAN list. Note that the gateway nodes in one data center will have connectivity by means of virtual tunnel end points (VTEPs), whereas gateway nodes must be able to handle EVPN-VXLAN encapsulation on the data center side and EVPN-MPLS on the WAN (data center interconnect) side.

  EVPN interconnect CLI commands:

```
set routing-instances <instance-name> protocols evpn interconnect interconnected-vlan-list
[ <vlan-id1> <vlan-id2>]
```

```
set routing-instances <instance-name> protocols evpn interconnect encapsulation mpls
```

  [See Technology Overview of VXLAN-EVPN Integration for DCI and Connecting Logical Systems Using Logical Tunnel Interfaces.]

High Availability

- **Unified ISSU support on EX4650**—Starting in Junos OS Release 21.4R1, EX4650 switches support unified in-service software upgrade (ISSU). The unified ISSU feature enables you to upgrade between two different Junos OS releases with minimal disruption on the control plane and with minimal disruption of traffic.

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

> **NOTE**: EX4650 switches provide unified ISSU support only if the Cancun versions of the chipset SDK are the same for the current version and the version you are upgrading to. See, No Link Title.

[See Getting Started with Unified In-Service Software Upgrade and Understanding In-Service Software Upgrade (ISSU).]

Additional Features

We've extended support for the following features to these platforms.

- **DHCP security** (EX9200, MX240, MX480, MX960, MX2010, MX2020). MPC10E line cards support the following DHCP security features:
  - DHCP snooping with Option 82.
  - DHCPv6 snooping with Option 16, Option 18, Option 37, and Option 79.
  - Lightweight DHCPv6 Relay Agent.

  [See DHCP Snooping.]
- **EVPN Type 2 and Type 5 route coexistence** (EX9200, EX9251, EX9253, MX204, MX240, MX480, MX960, MX2010, MX10003, MX10008, and QFX10002-60C)

  [See EVPN Type 2 and Type 5 Route Coexistence with EVPN-VXLAN.]
- **MACsec bounded delay protection** (EX4400 and SRX380)

  [See bounded-delay.]
- **Precision Time Protocol (PTP) transparent clock** (EX4300 and EX4300-48MP)

  [See PTP Transparent clocks.]
- **Support for OSPF, IS-IS, BGP, and static routing on IRB interfaces in EVPN-VXLAN networks** (EX4300-48MP and EX4400)

  [See Supported Protocols on an IRB Interface in EVPN-VXLAN.]
- **Support for IEEE 802.1ag CFM on service provider interfaces and Q-in-Q (point-to-point) interfaces** (EX2300, EX3400, EX4300, EX4300-48MP, and EX4400)

[See Introduction to OAM Connectivity Fault Management (CFM).]

- **Supported transceivers, optical interfaces, and DAC cables** (ACX Series, EX Series, PTX Series, MX Series, and QFX Series).—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

- What's Changed in Release 21.4R2 | 20
- What's Changed in Release 21.4R1 | 21

Learn about what changed in this release for EX Series switches.

What's Changed in Release 21.4R2

IN THIS SECTION

- General Routing | 20
- Network Management and Monitoring | 21
- User Interface and Configuration | 21

General Routing

- OpenConfig container names for Point-to-Multipoint per interface ingress and egress sensors are modified for consistency from "signalling" to "signaling".
- OpenConfig container names for Point-to-Multipoint per interface ingress and egress sensors are modified for consistency from "signalling" to "signaling".

Network Management and Monitoring

- Change in behavior of SNMP MIB object ifAlias?SNMP MIB object ifAlias now shows the configured interface alias. In earlier releases, ifAlias used to show configured interface description.
- **Changes when deactivating or deleting instances of the ephemeral configuration database** (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

User Interface and Configuration

- When you configure max-cli-sessions at the `edit system` hierarchy level, it restricts the maximum number of CLI sessions that can coexist at any time. Once the maximum-cli-sessions number is reached, new CLI access is denied. The users who are configured to get the CLI upon login, are also denied new login.

What's Changed in Release 21.4R1

IN THIS SECTION

- EVPN | 22
- General Routing | 22
- Interfaces and Chassis | 22
- Network Management and Monitoring | 22

EVPN

- **Output for show Ethernet switching flood extensive**—The output for show ethernet-switching flood extensive now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as unilist. Previously, the output for show ethernet-switching flood extensive would misidentify the next-hop type as composite.

General Routing

- **Juniper Agile Licensing (EX2300-VC, EX3400-VC, EX4300-VC, EX4400-24MP, EX4400-48MP, PTX10003, PTX10016, QFX5130-32CD, QFX5110-32Q, QFX5110-48S, QFX5120-48T, QFX5210-64C, QFX5200, and QFX5220)**—Starting from this release onwards, the Juniper Agile License Manager is deprecated. You can use the Juniper Agile Licensing Portal to activate, install, manage, and monitor licenses on Juniper Networks devices.

  [See Juniper Agile Licensing Guide.]

Interfaces and Chassis

- When configuring multiple flexible tunnel interface (FTI) tunnels, the source and destination address pair needs to be unique only among the FTI tunnels of the same tunnel encapsulation type. Prior to this PR, the source and destination address pair had to be unique among all the FTI tunnels regardless of the tunnel encapsulation type.

Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.

Known Limitations

IN THIS SECTION

General Routing | 23

- Infrastructure | 23

Learn about known limitations in Junos OS Release 21.4R2 for EX Series switches.

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

General Routing

- When the device is up and running for a long time, there is a possibility FS gets bad blocks and it is accumulated. When any change done to it, it reloads and tries to recover the bad blocks from the FS. PR910445
- Unified ISSU on QFX5120-48Y and EX4650 devices will not be supported if there is a change in the Cancun versions of the chipset SDKs between the releases. This is a product limitation as change in the Cancun firmware leads to the chip reset and hence unified ISSU is impacted. The Cancun versions in the chipset SDKs should be the same between two operating system releases for unified ISSU to work. PR1634695

Infrastructure

- While upgrading the image from 21.2 to 21.3, the `no-validate` configuration statement is mandatory for the upgrade command to proceed. PR1586481

Open Issues

IN THIS SECTION

- General Routing | 24
- Forwarding and Sampling | 26
- Infrastructure | 26

Network Management and Monitoring | 26
Platform and Infrastructure | 26

Learn about open issues in Junos OS Rlease 21.4R2 for EX Series switches.

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

General Routing

- When running the command show pfe filter hw filter-name <filter name>, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. PR1495712
- A delay of 35 seconds is added in reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. PR1514364
- The FPC process might not get spawned after hard reboot in a rare case, which causes the FPC to not come online successfully. PR1540107
- Pause frames counters are not getting incremented when pause frames are sent. PR1580560
- On EX4400 family of devices, sometimes login prompt is not shown after the login session ends. PR1582754
- In rare circumstances when doing routing-engine switchover, the routing protocol daemon in former active routing-engine (new backup routing-engine) might restart with a coredump while in process of being terminated.PR1589432
- On EX series devices with vendor chip as Packet Forwarding Engine (PFE), if IS-IS is enabled on an integrated routing and bridging (IRB) interface and the maximum transmission unit (MTU) size of the IRB interface is configured with a value great than 1496 bytes, the IS-IS hello (IIH) PDUs with jumbo frame size (i.e., great than 1496 bytes) might be dropped and not sent to the IS-IS neighbors. The following is the product list of EX series devices with vendor chip as Packet Forwarding Engine. EX2300, EX3400, EX4300, EX4600, and EX4650. PR1595823
- EX4400 platforms have a Cloud LED on the front panel to indicate the onboarding of the device to cloud (day0) and management after onboarding (day1). If MIST is used as a Management entity in cloud then, the cloud LED will display green in situations where device would have lost connectivity to cloud. This is dues to MIST using outbound SSH for management. This behavior is not applicable

to any other management entity which uses outbound https and LED will display appropriate states to indicate the loss on connection to cloud. PR1598948

- EX4400-48MP - VM cores and VC split might be observed with multicast scale scenario. PR1614145
- Issue: DHCP binding will not happen, when MLD snooping is enabled. Root cause: During DHCPv6 binding process, ICMPv6 neighbour discovery packets will be transacted between DHCP server device and client device tp learn adjacency. As per the design, ICMPv6 multicast packets will get dropped in DHCP security device and DHCPv6 binding will not happen as well. This issue is applicable only for Trinity based line cards and this is in parity with the older legacy Line cards. So, this config is not supported on this platform. DHCP-security vlan config: set vlans dhcp-vlan vlan-id 100 set vlans dhcp-vlan forwarding-options dhcp-security option-82 circuit-id set interfaces xe-0/1/3:1 unit 0 family ethernet-switching vlan members dhcp-vlan set interfaces xe-0/1/3:3 unit 0 family ethernet-switching interface-mode trunk set interfaces xe-0/1/3:3 unit 0 family ethernet-switching vlan members dhcp-vlan set interfaces xe-0/2/2:0 unit 0 family ethernet-switching interface-mode trunk set interfaces xe-0/2/2:0 unit 0 family ethernet-switching vlan members dhcp-vlan Committing MLD snooping on the vlan: set protocols mld-snooping vlan dhcp-vlan. PR1627690
- Mixing of GBP and non GBP terms in a single firewall filter is not supported and commit error is provided at CLI. PR1630982
- On EX4600 devices, show dot1x firewall output for clients authenticated in CP (after fallback) might show incorrect packet count.PR1636503
- On all EX3400 and EX4400 devices, the Virtual-Chassis (VC) port might not be formed automatically after executing the command `request system zeroize`.PR1649338
- The EX4300-48mp does not generate ICMPv6 too long messages causing path MTU discovery to fail. As a result IPv6 session establishment fails. Path MTU discovery (PMTUD) is mandatory for IPv6, when MTU discovery fails IPv6 session establishment also will fails. In customer side SSH fails to establish due to keys too big to be fragmented.PR1655654
- On a EX2300 and EX4400 device, while configuring access control lists, dfwd core might be observed. PR1656219
- When a EX4400 Virtual Chassis is upgraded to 21.4R2 release using non-stop image upgrade process, the Virtual Chassis might report a alarm indicating a Virtual Chassis member is having different software version though all members are running same software versions. This alarm will be cleared on subsequent reboot of the chassis.PR1658508
- The port/MAC gbp tags might not be carried forward to the spine. PR1659384

Forwarding and Sampling

- The **fast-lookup-filter** with match not supported in FLT hardware might cause the traffic drop. PR1573350

Infrastructure

- A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks operating system allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. PR1497768

Network Management and Monitoring

- A minor memory leak is seen in the event-daemon process when multiple GRES switchovers are performed. PR1602536

Platform and Infrastructure

- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect ASIC programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. PR1530160
- During Routing Engine switchover interface flap might be seen along with Scheduler slippage. PR1541772
- When a EX4400 Virtual Chassis is scaled with different features configurations and device is stressed with traffic, device might not respond for CLI commands for a short period of time and a vmcore might be reported at that time. Once VM core is saved, device will continue to operate normally. PR1599498
- During VCCP flaps, Packet Forwarding Engine socket might get closed due to Virtual Chassis disconnection, and core might be observed due to access of freed memory, as a side effect. Due to a race condition between ukern threads, some API might free a memory while it might be being accessed from other API.PR1655530

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.4R2 | 27
- Resolved Issues: 21.4R1 | 30

Learn about the issues fixed in this release for EX Series switches.

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

Resolved Issues: 21.4R2

IN THIS SECTION

- General Routing | 27
- Interfaces and Chassis | 29
- Junos Fusion Enterprise | 29
- Layer 2 Ethernet Services | 29
- MPLS | 30
- Platform and Infrastructure | 30
- Routing Protocols | 30
- Subscriber Access Management | 30
- Virtual Chassis | 30

General Routing

- Error message **sensord: Error updating RRD file: /var/run/sensord.rrd** might be seen on WRL9 based line card. PR1420927
- Error message **error: syntax error: request-package-validate** will be seen on device CLI output during Non Stop Software Upgrade. PR1596955

- The interface on SFP-T or SFP-SX might stop forwarding traffic on EX4600 devices. PR1598805
- On EX4300 platform MAC addresses aging issue is seen. PR1600029
- The SFP-T port might stop forwarding traffic on EX4600 devices. PR1600291
- Traffic stops when traffic is switching from one LAG member to another member in case of MACSEC is configured. PR1611772
- The FXPC core might be seen on some EX platforms. PR1613532
- FPC might crash after device restart in EVPN-VXLAN scenario. PR1613702
- Removing the optical module "JNP-SFPP-10GE-T" from a port might cause certain ports to go down. PR1614139
- Packet Forwarding Engine might crash due to deletion of storm control configuration for IFL in CLI which might lead to traffic loss. PR1616646
- The device will be unavailable while performing FIPS 140-2/FIPS 140-3 level 2 internal test on FreeBSD 12 based Junos OS platforms. PR1623128
- Traffic loss might be observed after configuring VXLAN over IRB interface. PR1625285
- When clients connected to isolated VLAN (Virtual Local Area Network) through trunk port cannot communicate to the network. PR1626710
- DHCP clients might not go to BOUND state when the aggregate Ethernet bundle is enabled between DHCP server and snooping device. PR1627611
- Packet drop might be observed when L2PT is configured on transit device. PR1627857
- On EX4650 devices running on Junos operating system, certain traffic received by the Junos OS device on the management interface might be forwarded to egress interfaces instead of discarded (CVE-2022-22186). PR1628754
- The error nessage **BCM_PVLAN_UTILS:ERR:pfe_bcm_pvlan_utils_get_sec_bd(),789: Failed to get Secondary-bd** is logged when received a DHCP packet on Private VLAN. PR1630553
- Unicast ARP packets with the first four bytes of its destination MAC matching to system MACs of a transit system gets trapped by the system. PR1632643
- Traffic loss for 20 seconds on VC with aggregate Ethernet link-protection when rebooting backup FPC. PR1633115
- The VCPs connected with the AOC cable might not come up after upgrading to 17.3 or later releases. PR1633998
- The FXPC process crash might be triggered when a MAC is aging out. PR1634433

- dot1x ports might be stuck in the connecting state after clearing the dot1x sessions. PR1634820
- IRB traffic drop might be observed when mac-persistence-timer expires. PR1636422
- Configuring L2PT on a transit switch in a Q-in-Q environment breaks L2PT for other S-VLANs. PR1637249
- MAC address might not be learned on the new interface after MAC move. PR1637784
- Delay might be observed for the interfaces to come up after reboot or transceiver replacement.PR1638045
- MAC-move might be observed when DHCP-security is configured. PR1639926
- The error nessage **dot1xd : devrt_rtsock Don't know how to handle message type 2** is logged even if dot1x is not set. PR1641304
- The VMcore might be observed on EX devices in rare scenario. PR1641988
- Traffic loop might occur due to STP ports not created in new primary Routing Engine after switchover due to reboot of primary Routing Engine on EX4300, EX3400, and EX2300 platforms in Virtual Chassis (VC) scenario. PR1647000
- The VCP link might take longer time to come up during system reboot/Packet Forwarding Engine restart. PR1651316
- On EX9251 devices, reboot reason shows as **0x2000:hypervisor reboot** instead of **0x4000:VJUNOS reboot** when we reboot the operating system. PR1651721

Interfaces and Chassis

- SNMP_TRAP_LINK_UP & SNMP_TRAP_LINK_DOWN trap might be seen while activating and deactivating firewall filters. PR1609838

Junos Fusion Enterprise

- JUNOS:JDI_FT_REGRESSION:PROTOCOLS:SWITCHING:SDPD:sdpd core with traces 0x0815e029 in vfpc_cascade_port_discovered,0x0817976d in csp_sd_device_discovered is seen on b54-rodnik2-sys. PR1555597

Layer 2 Ethernet Services

- Option 82 might not be attached on DHCP request packets. PR1625604
- DHCP packets might not be sent to the clients when `forward-only` is reconfigured under the routing instance. PR1651768

MPLS

- MPLS VPN packets drop due to missing ARP entry on PE. PR1607169

Platform and Infrastructure

- Some interfaces might be down after the power outage or power cycle. PR1580829
- VSTP might not work in Q in Q environment. PR1622404
- Traffic loss might be seen when the interface fails to verify the parameter LOCAL-FAULT. PR1623215
- The ARP resolution might get failed on VRRP enabled interface. PR1630616
- Application of firewall filters might break connectivity towards the hosts on EX4300 devices. PR1630935
- The Packet Forwarding Engine might get crash when VC member flaps on EX devices. PR1634781
- SCB reset with Error : zfchip_scan line = 844 name = failed due to PIO errors. PR1648850

Routing Protocols

- The rpd might crash and restart when NSR is enabled.. PR1620463

Subscriber Access Management

- Adding the new radius access configuration might fail. PR1629395

Virtual Chassis

- Delay might be observed while establishing the virtual-chassis post upgrading or rebooting device. PR1624850

Resolved Issues: 21.4R1

IN THIS SECTION

- General Routing | **31**
- Class of Service (CoS) | **34**
- EVPN | **34**

- Infrastructure | 34
- Interfaces and Chassis | 35
- Junos Fusion Enterprise | 35
- Layer 2 Ethernet Services | 35
- Platform and Infrastructure | 35
- Routing Protocols | 36
- Virtual Chassis | 36

General Routing

- CSPRNG is changed to the HMAC-DRBG and cannot be changed to either the FreeBSD Fortuna or the Juniper DYCE RNGs. PR1529574
- Junos 'et-' interface stuck and remains down between two particular ports PR1535078
- On EX Series line of switches Virtual Chassis (VC), Power over Ethernet (POE) might not be detected and hence might fail to work on VC members. PR1539933
- The Virtual Chassis Port (VCP) might not come up on EX4600 platform. PR1555741
- Some transmitting packets might get dropped due to the **disable-pfe** action is not invoked when the fabric self-ping failure is detected. PR1558899
- The DHCP client might not obtain IP address when dhcp-security is configured. PR1564941
- On EX platforms, the new primary Routing Engine post switchover might go into DB mode (or crash). PR1565213
- The MAC address will point to incorrect interface after traffic is stopped and not aging out. PR1565624
- The fxpc process might crash and cause traffic loss in the IFBD scenario. PR1572305
- Private VLAN configuration might fail in certain scenario. PR1574480
- Kernel crash migiht be observed on the backup Routing Engine after GRES. PR1577799
- The dcpfe crash is observed on Junos OS EX Series line of switches. PR1578859
- On EX Series line of switches, some 40G ports might not be channelized successfully. PR1582105
- The upgrade of the PoE firmware might fail on EX2300 and EX3400.PR1584491

- Packet drops during VRRP primary reboot when 40XS linecard is present on some EX9204 platforms. PR1586740
- Process dot1xd crash might be seen and re-authentication might be needed on EX9208 platform. PR1587837
- Inconsistent statistics value seen on performing **slaac-snooping**. PR1590926
- The DHCP relay might not work if it connects with the server via type 5 route which with aggregated Ethernet interface as the underlay interface. PR1592133
- On the EX4300-48MP Virtual Chassis, the backup Routing Engines clear the reporting alarm for a PEM failure intermittently for a missing power source. PR1593795
- Clients authentication failure might occur due to dot1x daemon memory leak. PR1594224
- On a EX4400 Virtual Chassis, log messages related to fan settings will be observed in chassis traceoptions file. PR1594446
- The label field for the EVPN Type 1 route is set to 1. PR1594981
- The MAC/IP withdraw route might be suppressed by rpd in the EVPN scenario. PR1597391
- The backup Virtual Chassis member might not learn MAC address on a primary after removing a VLAN unit from the SP style aggregated Ethernet interface which is part of multiple VLAN units. PR1598346
- On EX3400 platforms, traffic might fail to flow in MACsec enabled interfaces. PR1598610
- Error might be seen when enabling xSTP on all interfaces. PR1598839
- The l2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable PR1599094
- On EX4400 Virtual chassis, linecard member console might fail to redirect to Virtual Chassis primary. PR1599625
- Unable to disable the management port em1. PR1600905
- EX4400 PVIDB schema files not updated for the correct count of (lic_ft_cnt) Licensing feature. PR1601449
- On EX2300 and EX4650, if the system is upgraded from 20.2 or earlier release to 20.3 or later release, either using phone-home feature or when the system is in factory default state, the upgrade will fail with phone-home crash. PR1601722
- On EX2300 Virtual Chassis platforms ARP might not get resolved. PR1602003
- Files under **/var/db/scripts** might become inaccessible after every reboot. PR1602638

- On a EX4400 Virtual Chassis, the Cloud LED will display pattern for **NO_CLOUD_RESPONSE** when there is no IP address present on IRB interface or no DNS is configured on the device. PR1602664
- On EX4400 dot1x authentication might not work on EVPN/xlan enabled endpoints. PR1603015
- The fxpc core files are generated when the NSSU performed with MACsec configuration. PR1603602
- MAC move might be seen between the ICL and MC-LAG interface if adding or removing VLANs on the ICL interface. PR1605234
- On a EX4400 POE supported device, PoE firmware upgrade should be done with bt-firmware CLI option only. PR1606276
- In Junos OS releases, in a scenario with dhcp-security and option-82 configured, the jdhcpd crashes upon receipt of a malformed DHCP packet (CVE-2022-22176). PR1606794
- On EX Series switches, the fxpc process might crash and generate a core dump. PR1607372
- On EX4300 platform, the dcpfe process might crash and generate core. PR1608306
- DHCP packets might be received and then returned back to DHCP relay through the same interface on EX2300, EX3400, and EX4300 Virtual Chassis platforms. PR1610253
- Traffic loss might be observed if dot1X is configured with **supplicant multiple** and authenticated user from radius is in single supplicant mode. PR1610746
- Inter-vlan connectivity might be lost in an EVPN-VXLAN with CRB topology. PR1611488
- Change in commit error message while configuring the same vlan-id with different vlan-name through `openconfig` CLI. PR1612566
- On EX2300, EX3400, EX4300-MP, and EX4400 series is causing MAC move when the IGMP query packet received on backup FPC port. PR1612596
- FPC might crash after device restart in EVPN-VXLAN scenario. PR1613702
- EX9204 :: entAliasMappingIdentifier does not reflect correct SNMP entity to ifindex mapping for 100G and 40G ports. PR1614081
- After performing zeroize factory default configuration does not show appropriate interface in the device. PR1614098
- Removing the optical module **JNP-SFPP-10GE-T** from a port might cause certain ports to go down. PR1614139
- SFP+-10G-T-DWDM-ZR support for EX3400. PR1615246
- Core dumps might be seen on EX devices after configuration changes. PR1618352

- Lowest acceptable PN not reflecting correct value when replay-window-size is more than zero. PR1618598
- The process dcpfe might crash after performing VXLAN VNI configuration change and delete on EX series platforms. PR1619445
- In Junos OS releases, the EX2300 Series, EX2300-MP Series, EX3400 Series: A slow memory leak due to processing of specific IPv6 packets (CVE-2022-22180). PR1619970
- OAM CFM session doesn't come up if ERPS configured and CFM control traffic uses the same VLAN as ERPS control traffic. PR1620536
- EVPN type 5 routes might not be installed. PR1620808
- Traffic loss might be observed after configuring VXLAN over IRB interface. PR1625285
- The filter required for routing the Layer 3 traffic of targeted broadcast and static ARP entry with multicast-mac address might fail to install. PR1626620
- When clients connected to isolated VLAN (Virtual Local Area Network) through trunk port cannot communicate to the network. PR1626710

Class of Service (CoS)

- The dcpfe core might be seen in auto-channelization scenario or when SFP is plugged out. PR1616847

EVPN

- Traffic loss might be seen under EVPN scenario when MAC-IP moves from one CE interface to another. PR1591264
- Traffic loss might be seen if aggregated Ethernet bundle interface with ESI is disabled on primary Routing Engine followed by a Routing Engine switchover. PR1597300

Infrastructure

- For EX4400 product family, net installation (PXE) is not working. PR1577562
- EX2300, EX2300-MP, and EX3400 do not take kernel core file to internal storage on panic. PR1600442
- Upgrade might fail when upgrading from legacy release. PR1602005
- The fxpc process might crash and generate core. PR1611480

- DHCP packets originated from QinQ/SP VLANs will have vlan-id of C-vlan in DHCP options82 circuit-id field. Whereas when configured to use VLAN description, then S VLAN name will be used in circuit-id. PR1616613

Interfaces and Chassis

- ARP resolution failure might occur during VRRP failover. PR1578126
- The **SNMP_TRAP_LINK_UP** and **SNMP_TRAP_LINK_DOWN** trap might be seen while activating and deactivating firewall filters. PR1609838

Junos Fusion Enterprise

- Reverting primaryship from RE1 to RE0 might lead to l2ald daemon crash and cause an outage. PR1601817

Layer 2 Ethernet Services

- The DHCP client might be offline for about 120 seconds after sending the DHCPINFORM message. PR1587982
- The jdhcpd process started spiking and DHCP become unresponsive if modifying the configuration to add `override always-write-giaddr` and removed `forward-only`. PR1618306

Platform and Infrastructure

- FPC crashes might be seen on EX92 platforms. PR1579182
- HEAP malloc(0) is seen with base configurations. PR1590037
- Broadcast traffic might be discarded when a firewall filter is applied to the loopback interface. PR1597548
- VLAN tagged traffic might be dropped with service provider style configuration. PR1598251
- The VRRP packets might not be forwarded when **mac-move-limit** configuration statement is configured. PR1601005
- Adding aggregated Ethernet configuration without child member might cause MAC or ARP learning issues.PR1602399
- The ZTP service might not work and the image installation fails. PR1603227
- Slaac-Snooping global address entry learnt over vtep interface does not RENEW sometimes after lease timer expiry. PR1603269

- Route leak from primary routing-instance to custom routing-instance failure occurs for local interface. PR1623429

Routing Protocols

- The rpd core might be observed due to memory corruption. PR1599751
- The rpd might crash and restart when NSR is enabled. PR1620463

Virtual Chassis

- During NSSU, errors related to link might be observed while IFDs are attached are detached. PR1622283

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for EX Series switches.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 37

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

Starting in Junos OS release 21.4R2, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS except EX4400. EX4400 still runs on FreeBSD 11.x based Junos OS.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

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

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

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

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

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

Table 2: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for JRR Series

IN THIS SECTION

- What's New | 38
- What's Changed | 38
- Known Limitations | 39
- Open Issues | 39
- Resolved Issues | 39
- Documentation Updates | 40
- Migration, Upgrade, and Downgrade Instructions | 40

These release notes accompany Junos OS Release 21.4R2 for the JRR Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features or enhancements to existing features in Junos OS Release 21.4R2 and 21.4R1 for JRR Series Route Reflectors.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R2 and 21.4R1 for JRR Series Route Reflectors.

Known Limitations

There are no known limitations in hardware and software in Junos OS Release 21.4R2 for JRR Series Route Reflectors.

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

Open Issues

There are no known issues in hardware and software in Junos OS Release 21.4R2 for JRR Series Route Reflectors.

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

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.4R2 | 39
- Resolved Issues: 21.4R1 | 40

Learn which issues were resolved in the Junos OS main and maintenance releases for JRR Series.

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

Resolved Issues: 21.4R2

IN THIS SECTION

- General Routing | 40

General Routing

- The "monitor traffic interface" might not work for em2 on vRR/JRR200. PR1629242

Resolved Issues: 21.4R1

IN THIS SECTION

- General Routing | 40

General Routing

- On JRR200, incorrect Power Entry Module (PEM) load percentage is observed when you execute the `show chassis power` command. PR1598728

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for JRR Series Route Reflectors.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 41

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

For information about software installation and upgrade, see the JRR200 Route Reflector Quick Start and Installation and Upgrade Guide.

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

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

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

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

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

Table 3: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

- What's New | 42
- What's Changed | 43
- Known Limitations | 43
- Open Issues | 44
- Resolved Issues | 44
- Documentation Updates | 44

These release notes accompany Junos OS Release 21.4R2 for Juniper Secure Connect. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

- What's New in 21.4R2 | 42
- What's New in 21.4R1 | 43

Learn about new features introduced in the Junos OS main and maintenance releases for the Juniper Secure Connect.

What's New in 21.4R2

There are no new features or enhancements to existing features in Junos OS Release 21.4R2 for Juniper Secure Connect.

What's New in 21.4R1

IN THIS SECTION

- Authentication and Access Control | 43

Learn about new features introduced in this release for Juniper Secure Connect.

Authentication and Access Control

- **LDAP authentication for Juniper Secure Connect (SRX Series devices and vSRX with Juniper Secure Connect)**—In Junos OS Release 21.4R1, we've introduced support for native LDAP authentication with secure connection to simplify deployments of Juniper Secure Connect. With the LDAP authentication support, you can determine which groups should be granted access after successful authentication. Use the `address-assignment` option at the `[edit access profile profile-name authentication-order ldap ldap-options]` hierarchy level to assign IP addresses specifically for those groups of users to simplify IP address management.

  [See ldap-options.]

What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R2 and 21.4R1 for Juniper Secure Connect.

Known Limitations

There are no known limitations in hardware and software in Junos OS 21.4R2 for Juniper Secure Connect.

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

Open Issues

There are no known issues in hardware and software in Junos OS Release 21.4R2 for Juniper Secure Connect.

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

Resolved Issues

There are no resolved issues in Junos OS Release 21.4R2 and 21.4R1 for Juniper Secure Connect.

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

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for Juniper Secure Connect.

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

- What's New | 45
- What's Changed | 45
- Known Limitations | 45
- Open Issues | 45
- Resolved Issues | 46
- Documentation Updates | 46

- Migration, Upgrade, and Downgrade Instructions | 46

These release notes accompany Junos OS Release 21.4R2 for the Junos Fusion for enterprise. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features or enhancements to existing features in Junos OS release 21.4R2 and 21.4R1 for Junos fusion for enterprise.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R2 and 21.4R1 for Junos Fusion for enterprise.

Known Limitations

There are no known limitations in hardware and software in Junos OS 21.4R2 for Junos fusion for enterprise.

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

Open Issues

There are no open issues in hardware and software in this release for Junos Fusion for enterprise.

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

Resolved Issues

There are no resolved issues in the Junos OS main and maintenance releases for Junos Fusion for enterprise.

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

Documentation Updates

There are no errata or changes in JJunos OS Release 21.4R2 and 21.4R1 for Junos Fusion for enterprise documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Basic Procedure for Upgrading Junos OS on an Aggregation Device | **47**
- Upgrading an Aggregation Device with Redundant Routing Engines | **48**
- Preparing the Switch for Satellite Device Conversion | **49**
- Converting a Satellite Device to a Standalone Switch | **51**
- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of- Life Releases | **51**
- Downgrading Junos OS | **51**

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

Basic Procedure for Upgrading Junos OS on an Aggregation Device

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

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

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

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

To download and install Junos OS:

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

   https://www.juniper.net/support/downloads/

2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

3. Select **By Technology > Junos Platform > Junos fusion** to find the software that you want to download.

4. Select the release number (the number of the software version that you want to download) from the Version drop-down list on the right of the page.

5. Select the **Software** tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

9. Copy the software to the routing platform or to your internal software distribution site.

10. Install the new `junos-install` package on the aggregation device.

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

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

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

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

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

Replace *source* with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

For the detailed procedure, see the *Installation and Upgrade Guide*.

Preparing the Switch for Satellite Device Conversion

There are multiple methods to upgrade or downgrade satellite software in your Junos fusion for enterprise. See Configuring or Expanding a Junos fusion for enterprise.

For satellite device hardware and software requirements, see Understanding Junos fusion for enterprise Software and Hardware Requirements.

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

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

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

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

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

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

2. Clear the device:

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Switch

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

Upgrade and Downgrade Support Policy for Junos OS Releases 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 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

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

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

Downgrading Junos OS

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

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

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

Junos OS Release Notes for Junos Fusion for Provider Edge

IN THIS SECTION

- What's New | 52
- What's Changed | 53
- Known Limitations | 53
- Open Issues | 53
- Resolved Issues | 53
- Documentation Updates | 53
- Migration, Upgrade, and Downgrade Instructions | 54

These release notes accompany Junos OS Release 21.4R2 for Junos Fusion for Provider Edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features or enhancements to existing features in Junos OS Release 21.4R2 and 21.4R1 for Junos Fusion for Provider Edge.

What's Changed

There are no changes in behavior and syntax in Junos OS Releases 21.4R2 or 21.4R1 for Junos Fusion for Provider Edge.

Known Limitations

There are no known limitations in hardware and software in Junos OS 21.4R2 for Junos fusion for provider edge.

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

Open Issues

There are no known issues in hardware and software in Junos OS Release 21.4R2 for Junos Fusion for Provider Edge.

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

Resolved Issues

There are no resolved issues in Junos OS Release 21.4R2 and 21.4R1 for Junos Fusion for Provider Edge.

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

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for Junos Fusion for Provider Edge.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Basic Procedure for Upgrading an Aggregation Device | 54
- Upgrading an Aggregation Device with Redundant Routing Engines | 57
- Preparing the Switch for Satellite Device Conversion | 57
- Converting a Satellite Device to a Standalone Device | 59
- Upgrading an Aggregation Device | 62
- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of- Life Releases | 62
- Downgrading from Junos OS Release 21.4 | 63

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

Basic Procedure for Upgrading an Aggregation Device

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

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

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

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates

and shell scripts (the only exceptions are the `juniper.conf` and `ssh` files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. See the Installation and Upgrade Guide.

The download and installation process for Junos OS Release 21.4R2 is different from that for earlier Junos OS releases.

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

   https://www.juniper.net/support/downloads/

2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

3. Select **By Technology > Junos Platform > Junos fusion** to find the software that you want to download.

4. Select the release number (the number of the software version that you want to download) from the Version drop-down list to the right of the page.

5. Select the **Software** tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

9. Copy the software to the routing platform or to your internal software distribution site.

10. Install the new `jinstall` package on the aggregation device.

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

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

    - For 64-bit software:

> **NOTE**: We recommend that you use 64-bit Junos OS software when implementing Junos fusion for provider edge.

```
user@host> request system software add validate reboot source/jinstall64-21.4R1.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.4R1.SPIN-domestic-signed.tgz
```

All other customers, use the following commands.

- For 64-bit software:

> **NOTE**: We recommend that you use 64-bit Junos OS software when implementing Junos fusion for provider edge.

```
user@host> request system software add validate reboot source/jinstall64-21.4R1.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.4R1.SPIN-export-signed.tgz
```

Replace *source* with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 21.4R2 `jinstall` package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the `jinstall` package that corresponds to the previously installed software.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

For the detailed procedure, see the *Installation and Upgrade Guide*.

Preparing the Switch for Satellite Device Conversion

Satellite devices in a Junos fusion topology use a satellite software package that is different from the standard Junos OS software package. Before you can install the satellite software package on a satellite device, you first need to upgrade the target satellite device to an interim Junos OS software version that

can be converted to satellite software. For satellite device hardware and software requirements, see Understanding Junos fusion Software and Hardware Requirements

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

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

Customers with EX4300 switches, use the following command:

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

Customers with QFX5100 switches, use the following command:

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

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

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

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

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

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

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

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

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

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

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

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

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, and preconfiguration. See Configuring Junos fusion for provider edge for detailed configuration steps for each method.

Converting a Satellite Device to a Standalone Device

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

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

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

1. Using a Web browser, navigate to the Junos OS software download URL on the Juniper Networks webpage:

https://www.juniper.net/support/downloads

2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

3. Select **By Technology > Junos Platform > Junos fusion** from the drop-down list and select the switch platform series and model for your satellite device.

4. Select the Junos OS Release 14.1X53-D30 software image for your platform.

5. Review and accept the End User License Agreement.

6. Download the software to a local host.

7. Copy the software to the routing platform or to your internal software distribution site.

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

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

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

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

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

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

9. Commit the configuration.

   To commit the configuration to both Routing Engines:

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

Otherwise, commit the configuration to a single Routing Engine:

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

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

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

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

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

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

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

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

11. Wait for the reboot that accompanies the software installation to complete.

12. When you are prompted to log back into your device, 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 21.4R2, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

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

We have two types of releases, EOL and EEOL:

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

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

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

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

Table 4: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Downgrading from Junos OS Release 21.4

To downgrade from Release 21.4 to another supported release, follow the procedure for upgrading, but replace the 21.4 `jinstall` package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for MX Series

IN THIS SECTION

- What's New | **64**
- What's Changed | **86**
- Known Limitations | **90**
- Open Issues | **94**
- Resolved Issues | **107**
- Documentation Updates | **138**
- Migration, Upgrade, and Downgrade Instructions | **138**

These release notes accompany Junos OS Release 21.4R2 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

- What's New in 21.4R2 | 64
- What's New in 21.4R1 | 64

Learn about new features introduced in this release for MX Series routers.

What's New in 21.4R2

There are no new features or enhancements to existing features in this release for the MX Series routers.

What's New in 21.4R1

IN THIS SECTION

- Hardware | 65
- Architecture | 74
- Chassis | 75
- EVPN | 75
- High Availability | 76
- IP Tunneling | 76
- Junos Telemetry Interface (JTI) | 76
- Layer 2 VPN | 76
- Interfaces | 77
- MPLS | 77
- Multicast | 77
- Network Address Translation (NAT) | 77
- Operation, Administration, and Maintenance (OAM) | 78
- Platform and Infrastructure | 78
- Routing Protocols | 79

- Source Packet Routing in Networking (SPRING) or Segment Routing | **79**
- Services Applications | **80**
- Software Defined Networking (SDN) | **80**
- Software Installation and Upgrade | **80**
- Subscriber Management and Services | **82**
- VPNs | **83**
- Additional Features | **84**

Learn about new features or enhancements to existing features in Junos OS Release 21.4R1 for the MX Series routers.

Hardware

- **New MX10K-LC9600 line card and JNP10008-SF2 Switch Fabric Board on MX10008**—Starting in Junos OS Release 21.4R1, we introduce the MX10K-LC9600 and SFB2 JNP10008-SF2. MX10K-LC9600 is a fixed-port line card that can deliver a bandwidth of up to 9.6 Tbps. The line card has twenty-four QSFP ports, each capable of supporting a maximum speed of 400 Gbps. MX10K-LC9600 interoperates with existing MX Series line cards, such as MX10K-LC2101 and MX10K-LC480 and interfaces with only JNP10008-SF2.
  JNP10008-SF2 is a ZF ASIC based Switch Fabric Board which provides the fabric interface required to meet line rate throughput of 9.6 Tbps. JNP10008-SF2 interfaces with MX10K-LC2101, MX10K-LC480, and MX10K-LC9600 line cards.

  [See Protocols and Application supported by the MX10K-LC9600.]

  Table 5 on page 66 summarizes the descriptions of the features supported on MX10K-LC9600 platform in Junos OS Release 21.4R1.

Table 5: Features supported on MX10K-LC9600

Feature	Description
Chassis	• In Junos OS Release 21.4R1, the MX10008 supports MX10K-LC9600, which is a fixed-port line card. However, the router supports the line card only if it also has the Switch Fabric Board SFB2 installed. The Joule fan trays and the Joule PSMs are required for SFB2 and MX10K-LC9600 support. Hyper mode is a default mode for SFB2 and MX10K-LC9600 line card. [See Fabric-Plane-Management-on-MX10008-Devices.] • In Junos OS Release 21.4R1, the Switch Fabric Board SFB2 on the MX10008 router supports the MX10K-LC2101, MX10K-LC480, and MX10K-LC9600 line cards. The Joule fan trays and the Joule PSMs are required for SFB2 and MX10K-LC9600 support. Hyper mode is a default mode for SFB2 and MX10K-LC9600 line card. No fabric redundancy is supported with MX10K-LC9600. For MX10K-LC2101 and MX10K-LC480 line cards, 5+1 SFB2 fabric redundancy is provided. [See Fabric-Plane-Management-on-MX10008-Devices.]
Class of Service (CoS)	• Forwarding Class of Service (CoS) and Hierarchical Class of Service (CoS) support [See Understanding Class of Service, and Hierarchical Class of Service for Subscriber Management Overview.]
Distributed Denial-of-Service (DDoS)	• Distributed Denial-of-Service (DDoS) Protection support—Supports DDoS protection, which is enabled by default. [See Control Plane Distributed Denial-of-Service (DDoS) Protection Overview.]
EVPN	• Support for EVPN-VXLAN Unicast features [See Understanding Programmable Flexible VXLAN Tunnels.] • Support for EVPN-MPLS Unicast and Multicast Forwarding features [See EVPN User Guide.]
Firewall Filter	• Enhanced firewall filter processing [See Understanding Firewall Filter Match Conditions.]

Table 5: Features supported on MX10K-LC9600 *(Continued)*

Feature	Description
Hardware	• New MX10K-LC9600 MPC—In Junos OS Release 21.4R1, we introduce the MX10K-LC9600 MPC, a fixed-configuration 24-port line card, which provides a line rate throughput of 9.6 Tbps. The MX10K-LC9600 has twenty-four QSFP ports, each capable of supporting a maximum speed of 400 Gbps. [See Protocols and Application supported by the MX10K-LC9600.] • New JNP10008-SF2 Switch Fabric Board—In Junos OS Release 21.4R1, we introduce the JNP10008-SF2, a ZF ASIC based Switch Fabric Board which provides the fabric interface required to meet line rate throughput of 9.6 Tbps utilizing the PAM4 signalling technology. JNP10008-SF2 interfaces with MX10K-LC2101, MX10K-LC480, and MX10K-LC9600 line cards. [See Protocols and Application supported by the MX10K-LC9600.]

High Availability (HA)	• Support for Bidirectional Forwarding Detection (BFD)—
	
	  • Centralized, Distributed, Inline, Single-hop, Multi-hop, and Micro BFD.
	
	  • BFD over integrated routing and bridging (IRB) interfaces.
	
	  • BFD over pseudowire over logical tunnel and redundant logical tunnel interfaces.
	
	  • Virtual circuit connectivity verification (VCCV) BFD for Layer 2 VPNs, Layer 2 circuits, and virtual private LAN service (VPLS).
	
	[See Understanding BFD for Static Routes for Faster Network Failure Detection, and Bidirectional Forwarding Detection (BFD).]
	
	• Resiliency support for Packet Forwarding Engine (PFE) and Switch Fabric Board (SFB) 2
	
	[See show system errors active.]

Table 5: Features supported on MX10K-LC9600 *(Continued)*

Feature	Description
Interfaces	• Interface support—MX10K-LC9600 is a fixed-port line card that can deliver a bandwidth of up to 9.6 Tbps. MX10K-LC9600 interoperates with existing MX Series line cards, such as MX10K-LC2101 and MX10K-LC480. The MX10K-LC9600 supports 12 Packet Forwarding Engines, each providing a maximum bandwidth of up to 800 Gbps. The line card supports six PICs, with four ports per PIC. Each port supports 10-Gbps, 25-Gbps, 40-Gbps, 100-Gbps, and 400-Gbps interface speeds using different optics. You can channelize the interfaces as follows: • Four 10 GbE interfaces • Four 25 GbE interfaces • Two 100 GbE interfaces • Four 100 GbE interfaces You can configure the port speed at the `[edit chassis]` hierarchy level. [See Port Speed.] • Optics support— Supports transceivers, optical interfaces, and direct attach copper (DAC) cables on MX10K-LC9600. [See Hardware Compatibility Tool, and optics-options.] • Load balancing support— • Enhanced hash key options. • Consistent flow hashing, source IP only hashing, and destination IP only hashing. • Symmetrical load balancing over 802.3 and LAGs. [See Understanding Per-Packet Load Balancing.]

Table 5: Features supported on MX10K-LC9600 *(Continued)*

Feature	Description
IP Tunneling	• Support for IP-in-IP tunnel encapsulation in IPv4 and IPv6 [See Configuring IP Tunnel Interfaces, and encapsulation.] • MX10K-LC9600 line card supports tunnel servicing [See Tunnel Services Overview.]
Junos Fusion Provider Edge	• MX10K-LC9600 interoperability with Junos fusion for provider edge [See Junos Fusion Provider Edge Overview.]

Table 5: Features supported on MX10K-LC9600 *(Continued)*

Feature	Description

Junos Telemetry Interface	• Logical interface statistics for IPv4 and IPv6 family input and output counters support
	
	[See Telemetry Sensor Explorer.]
	
	• CoS JTI sensor support —In Junos OS Release 21.4R1, JTI supports CoS sensors to export statistics by means of gRPC from a switch to a collector in the following areas:
	
	  • LP, HP, red drop packets, queued packets, and queued bytes for physical interfaces
	
	  • CoS interface-set description
	
	  • CoS forwarding class to queue mapping information
	
	  Use the following resource paths to export interface queue statistics:
	
	  • */junos/system/linecard/interface/queue/extended-stats/*
	
	  • */interfaces/interface/state/counters/out-queue/lp-red-drop-pkts*
	
	  • */interfaces/interface/state/counters/out-queue/hp-red-drop-pkts*
	
	  • */interfaces/interface/state/counters/out-queue/queued-pkts*
	
	  • */interfaces/interface/state/counters/out-queue/queued-bytes*
	
	  Use the resource path */qos/interfaces/interface/state/interface-id* to export the CoS interface-set description.
	
	  Use the resource paths */qos/forwarding-groups/forwarding-group/state/name* and */qos/forwarding-groups/forwarding-group/state/output-queue* to export forwarding class to queue statistics.
	
	  [See Telemetry Sensor Explorer.]
	
	• Platform sensors— We support:
	
	  • Chassis management error (cmerror) configuration and counters
	
	  • Fabric, optical, and FPC environment statistics

Table 5: Features supported on MX10K-LC9600 *(Continued)*

Feature	Description
	• Platform, interface, and alarm statistics • Transceiver statistics [See Telemetry Sensor Explorer and Junos Telemetry Interface User Guide.] • Junos telemetry interface (JTI) CPU and network processing unit (NPU) sensors support [See Understanding OpenConfig and gRPC on Junos Telemetry Interface, and Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).] • SR-TE statistics for uncolored SR-TE policies streaming on JTI [See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface), source-packet-routing, and show spring-traffic-engineering.]
Layer 2 features	• Layer 2 features support [See Configuring Q-in-Q Tunneling and VLAN Q-in-Q Tunneling and VLAN Translation, Understanding Layer 2 Bridge Domains, Understanding Layer 2 Learning and Forwarding, and Introduction to OAM Connectivity Fault Management (CFM).]
Layer 3 features	• Forwarding Layer 3 Routing features support [See Understanding OSPF Configurations, and BGP Overview.] • Layer 3 features support [See MPLS Overview, Multicast Overview, and Understanding Next-Generation MVPN Control Plane.]
Layer 3 VPN Tunnels	• Support for GRE and UDP key on dynamic (ephemeral) tunnels [See dynamic-tunnels, and dynamic-tunnel-gre-key.]
MACsec	• Support for Media Access Control Security (MACsec), including AES-256 encryption, extended packet numbering, and fail-open mode [See Configuring Media Access Control Security (MACsec) on Routers .]

Table 5: Features supported on MX10K-LC9600 *(Continued)*

Feature	Description

MPLS	• Support for Seamless MPLS Layer 2 and Layer 3 features—
	  • Layer 2 features: Pseudowire Headend Termination (PWHT).
	  • Layer 3 features: Redundant logical tunnel interfaces and Pseudowire subscriber interfaces using either logical tunnel or redundant logical tunnel interfaces as anchor point.
	[See Layer 2 VPNs and VPLS Feature Guide for Routing Devices, Redundant Logical Tunnels Overview, and Pseudowire Subscriber Logical Interfaces Overview.]
	• Support for MPLS features—
	  • Layer 2 and Layer 3 VPN
	  • Layer 2 circuit and Circuit cross-connect (CCC)
	  • 6PE and 6vPE
	[See Configuring Ethernet over MPLS (Layer 2 Circuit), and IPv6-over-Ipv4 Tunnels.]

Multicast	• Auto LSP Policer support—
	  • Multicast load balancing of point-to-multipoint label-switched-paths (LSPs) over aggregated Ethernet child links.
	  • Automatic policers for MPLS point-to-multipoint LSPs.
	  • Display of packet and byte statistics for sub-LSPs of a point-to-multipoint LSP.
	  • GRES and graceful restart for MPLS point-to-multipoint LSPs.
	  • Multicast virtual private network (MVPN) extranet or overlapping functionality.
	[See Example: Configuring Multicast Load Balancing over Aggregated Ethernet Links, and Point-to-Multipoint LSP Configuration

Table 5: Features supported on MX10K-LC9600 *(Continued)*

Feature	Description
Network Management and Monitoring	• Support for Port Mirroring [See Configuring Port Mirroring on M, T MX, ACX, and PTX Series Routers.]
Routing Policy and Firewall Filters	• Support for forwarding firewall [See Understanding Firewall Filter Match Conditions, Overview of Policers, Fast Update Filters Overview, Service Filter Overview, and Understanding Firewall Filter Fast Lookup Filter.] • Support for coexistence of source IP hash with consistent hash on [See Configuring Load Balancing Using Source or Destination IP Only, and Configuring Consistent Load Balancing for ECMP Groups.]

Table 5: Features supported on MX10K-LC9600 *(Continued)*

Feature	Description

Services Applications	• Inline Services support—
	  • Inline NAT- NAT44 and NPTv6
	  • Inline softwires- MAP-E and 6rd
	  • Inline J-flow
	  • Inline Monitoring
	  • Video Monitoring
	  • FlowTapLite
	  [See Inline NAT, Configuring Mapping of Address and Port with Encapsulation (MAP-E), Configuring Inline 6rd, and Monitoring, Sampling, and Collection Services Interfaces User Guide.]
	• Support for RFC 2544-based benchmarking tests
	  [See Understanding RFC2544-Based Benchmarking Tests on MX Series Routers.]
	• Support for Two-Way Active Measurement Protocol (TWAMP) and Real-Time Performance Monitoring (RPM)
	  [See Understand Two-Way Active Measurement Protocol, and Real-Time Performance Monitoring.]

Software Installation and Upgrade	• Support for Secure Boot [See Secure Boot.]
Subscriber Management and Services	• Subscriber services uplink support [See Protocols and Application supported by the MX10K-LC9600.]

Architecture

- **Support for UPF N9 uplink classifier (MX240, MX480, MX960, MX10003, and MX204 Routers)**—Starting in Junos OS Release 21.4R1, you can use the uplink classifiers functionality supported by the

control and user plane separation (CUPS)-enabled UPF (User Plane Functions) to do the following selectively on the link connected to your devices:

- Forward uplink traffic towards different protocol data unit (PDU) session anchors.
- Merge downlink traffic from the different PDU session anchors.

[See Junos Multi-Access User Plane Overview and CUPS Session Creation and Data Flow with Junos Multi-Access User Plane.]

Chassis

EVPN

- **Support for EVPN routing policies on the MPC10E and MPC11E (MX240, MX480, MX960, MX2010, and MX2020)**—Starting in Junos OS Release 21.4R1, Junos OS supports policy filter configurations for EVPN routes on the MX240, MX480, and MX960 routers with the MPC10E line cards and on the MX2010 and MX2020 routers with the MPC11E line cards. You can create policies and apply policy filters to import and export EVPN routes at a specific EVPN routing-instance level or at the BGP level if you want to apply the policy to all EVPN routing instances.

  [See Routing policies for EVPN.]

- **Interconnecting EVPN-VXLAN data centers with EVPN-MPLS in a WAN using gateway nodes (MX-Series, EX9200, EX9252, EX9253)**—Starting in Junos OS Release 21.4R1, you can interconnect EVPN-VXLAN data centers with EVPN-MPLS in a WAN using gateway nodes, but without using logical tunnel interfaces. In Release 21.4R1, you can interconnect only those BDs/VLANs that are on the interconnected VLAN list. Note that the gateway nodes in one data center will have connectivity by means of virtual tunnel end points (VTEPs), whereas gateway nodes must be able to handle EVPN-VXLAN encapsulation on the data center side and EVPN-MPLS on the WAN (data center interconnect) side.

  EVPN interconnect CLI commands:

```
set routing-instances <instance-name> protocols evpn interconnect interconnected-vlan-list
[ <vlan-id1> <vlan-id2>]
```

```
set routing-instances <instance-name> protocols evpn interconnect encapsulation mpls
```

  [See Technology Overview of VXLAN-EVPN Integration for DCI and Connecting Logical Systems Using Logical Tunnel Interfaces.]

High Availability

- **Unified ISSU with enhanced mode supported on MPC11E sub-line cards (MX2010 and MX2020)**—Starting in Junos OS Release 21.4R1, MX Series routers with MPC11E sub-line cards installed can use the enhanced mode ISSU option. Enhanced mode eliminates packet loss during the unified ISSU process.

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

  [See How to Use Unified ISSU with Enhanced Mode and Sub Line Card Overview.]

IP Tunneling

- **Support for unicast IP-over-IP (IP-IP) tunneling for IPv4 and IPv6 traffic signaled by BGP (MX960 and MX2008)**—Starting in Junos OS Release 21.4R1, we support an IP-IP encapsulation to facilitate IP overlay construction over an IP transport network.

  [See Overview of Next-Hop-Based Dynamic Tunneling Using IP-Over-IP Encapsulation]

Junos Telemetry Interface (JTI)

- **Streaming queue statistics for static demux interfaces over aggregated Ethernet interfaces (MX Series)**—Starting in Junos OS Release 21.4R1, we support streaming of quality-of-service (QoS) queue statistics using JTI for statically configured demux interfaces over aggregated Ethernet interfaces.

  [See Enabling Export of Subscriber Statistics and Queue Statistics for Dynamic Interfaces and Interface-Sets .]

Layer 2 VPN

- **Support for VPLS over transport class tunnels (MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, and vMX)**—Starting in Junos OS Release 21.4R1, you can configure VPLS (FEC129, BGP, and LDP) services on segment routing–traffic engineering (SR-TE), RSVP-TE, flexible algorithm, and BGP Labeled Unicast (BGP-LU) traffic tunnels. Junos OS supports both colored and non-colored routing configurations.

  [See Introduction to Configuring VPLS and BGP Classful Transport Planes Overview.]

Interfaces

- **New CLI command to view load-balancing statistics for af interfaces (MX480, MX960, MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 21.4R1, use the `show interfaces lb-stats *af-interface-name*` command at the guest network function (GNF) level to view the information about the load balancing of transmit traffic on each peer Packet Forwarding Engine of an abstracted fabric (af) interface. You can also view the statistics of the transmit traffic on the fabric queues (high and low queues) for each peer Packet Forwarding Engine on an af interface. In Junos OS releases earlier than Release 21.4R1, you use the `show interface *af-name*` command to display the load-balancing information.

  [See show interfaces lb-stats af.]

MPLS

- **Support for new statement `no-normalize-same-members` to resize member LSPs (MX Series and PTX Series)**—In Junos OS Release 21.4R1, we've added the `no-normalize-same-members` statement to the container LSP normalization configuration under the `[edit protocols mpls container-label-switched-path *NAME* splitting-merging]` hierarchy. When you enable the `no-normalize-same-members` configuration, you only resize the existing member LSPs with equal bandwidth. In earlier Junos OS releases, if normalization does not need to create or delete any member LSPs, you resignal the member LSPs with equal bandwidth.

  [See splitting-merging.]

Multicast

Network Address Translation (NAT)

- **Enhancements to source NAT pool IP address range and NAT pool name character length (SRX Series and MX-SPC3)**—Starting in Junos OS Release 21.4R1, we've increased the source NAT pool IP address range from 8 IP addresses to 64 IP addresses.

  We've also increased the configurable length of the source NAT pool name, destination NAT pool name, source NAT rule name, destination NAT rule name, static NAT rule name, and rule set name from 31 characters to 63 characters.

  [See show security nat source rule, show security nat destination rule, and show security nat static rule.]

Operation, Administration, and Maintenance (OAM)

- **Enhancements to Bidirectional Forwarding Detection (BFD)-triggered fast reroute (FRR) for unicast next hops and session-id-change-limiter-indirect (MX Series, PTX1000, PTX3000, PTX5000, PTX10001, PTX10002, PTX10016, QFX10002-60C, QFX10002, QFX10008, QFX10016, and vMX)**—In Junos OS Release 21.4R1, we've enhanced the BFD-triggered fast reroute (FRR) for unicast next hops and session-id-change-limiter-indirect to address the issue of traffic being silently discarded because of a session mismatch between the control plane and data plane.

  To limit the re-programming of the number of parent nodes of the indirect-nexthop and avoid additional the complexity in the Packet Forwarding Engine when the session-identifier id of the indirect nexthop is changed, use the `session-id-change-limiter-indirect` configuration statement at the `[edit routing-options]` hierarchy level.

  [See Bidirectional Forwarding Detection (BFD) for MPLS.]

Platform and Infrastructure

- **PKI usability enhancements (MX240, MX480, MX960, SRX Series, and vSRX)**—Starting in Junos OS Release 21.4R1, we've enhanced PKI commands to provide additional details about the local and certificate authority (CA)-issued certificates. With these enhancements, you can:

  - View the CA certificate status of a CA profile group using the `request security pki ca-profile-group-status ca-group-name` *`group-name`* command. See request security pki ca-profile-group-status.

  - Configure certificate automatic reenrollment trigger time in days, hours, or percentage using the `set security pki auto-re-enrollment cmpv2 certificate-id certificate-id-name re-enroll-time (days` *`value`*`| hours` *`value`*`| percentage` *`value`*`)` or `set security pki auto-re-enrollment scep certificate-id certificate-id-name re-enroll-time (days` *`value`*`| hours` *`value`*`| percentage` *`value`*`)` command. See auto-re-enrollment.

  - View the CA chain, SHA256 fingerprint, and certificate serial number (hexadecimal and decimal format) for a local certificate using the `show security pki local certificate <`*`cert_id`*`> detail` command. See show security pki local-certificate (View).

  - View the CA profile associated with a CA certificate and SHA256 fingerprint using the `show security pki ca-certificate <brief|detail>` command. See show security pki ca-certificate (View).

  - View additional verification information about local and CA certificate using the `request security pki local-certificate verify` and the `request security pki ca-certificate verify` command, respectively. See request security pki ca-certificate verify (Security) and request security pki local-certificate verify (Security).

  - View more PKI-related statistics using the `show security pki statistics` command. Clear the PKI statistics using the `clear security pki statistics` command. See show security pki statistics and clear security pki statistics.

- **Support for optics (MX10008 and MX10016)**—Starting in Junos OS Release 21.4R1, we've added SFP+-10G-T-DWDM-ZR in supported list of optics on the MX10K-LC480 line card.

  [See Hardware Compatibility Tool.]

Routing Protocols

- **Support for accepting BGP routes with `accept-own` community (MX480 and MX960)**—Starting in Junos OS Release 21.4R1, MX480 and MX960 routers accept BGP routes with the `accept-own`community, defined by *RFC 7611, BGP ACCEPT_OWN Community Attribute*.

  The feature enhances the interoperability of a Juniper router by enabling it to accept routes whose `ORIGINATOR_ID` or `NEXT_HOP` value matches that of the receiving BGP speaker. For example, when a provider edge (PE) device advertises routes with the route distinguisher of a source VRF, the route reflector attaches the `accept-own` community and re-advertises the routes back to the originator. The provider edge (PE) device can then import the routes into the other destination VRFs, excluding its own.

  [See BGP accept-own Community and accept-own.]

- **OSPF link delay measurement and advertising (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.4R1, you can measure and advertise various performance metrics in IP networks with scalability through probe messages that are sent by Two-Way Active Measurement Protocol (TWAMP) Light. OSPF receives probe messages and the measured values from TWAMP Light. OSPF advertises these messages as TLVs in packets. You can use these metrics to make path-selection decisions based on the network performance.

  [See How to Enable Link Delay Measurement and Advertising in OSPF.]

- **Support for FAD and FAPM on traffic engineering database and BGP-LS (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.4R1, we support FlexAlgo Definition (FAD) and FlexAlgo Prefix Metric (FAPM) on the traffic engineering database and BGP Link State (BGP-LS). You can store FAD and FAPM entries in the traffic engineering database and BGP-LS. You can also store multiple prefix segment identifiers (SIDs) for a prefix in BGP-LS. You can import the FAD and FAPM entries from the traffic engineering database to BGP-LS and export the FAD entries from BGP-LS to the traffic engineering database.

  [See What is Flexible Algorithm Definition (FAD).]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Support for SRv6 LSPs in PCEP (MX Series)**—Support for SRv6 LSP in PCEP (MX Series)- Starting Junos OS Release 21.4R1, all types of SRv6 LSPs, such as PCE-Initiated, locally created, and delegated SRv6 LSPs are supported in the Path Computation Element Protocol (PCEP).

[See SRv6 LSPs in PCEP.]

Services Applications

- **Support for GeoIP filtering, global allowlist, and global blocklist (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.4R1, you can configure the Security Intelligence process ipfd on the listed MX Series routers to fetch GeoIP feeds from Policy Enforcer. The GeoIP feeds help prevent devices from communicating with IP addresses belonging to specific countries.

  You can define:

  - A profile to dynamically fetch GeoIP feeds. Include the `geo-ip rule match country` *`country-name`* statement at the `[edit services web-filter profile` *`profile-name`* `security-intelligence-policy]` hierarchy level.
  - A template to dynamically fetch GeoIP feeds. Include the `geo-ip rule match group` *`group-name`* statement at the `[edit services web-filter profile` *`profile-name`* `url-filter-template` *`template-name`* `security-intelligence-policy]` hierarchy level.

  You can define a global allowlist by configuring the `white-list (IP-address-list |` *`file-name`*`)` statement at the `edit services web-filter profile` *`profile-name`* `security-intelligence-policy` hierarchy level. You can define a global blocklist by configuring the `black-list (IP-address-list |` *`file-name`*`)` statement at the `edit services web-filter profile` *`profile-name`* `security-intelligence-policy` hierarchy level. Here, *IP-address-list* refers to the name of the list specified at the `[edit services web-filter]` hierarchy level. The *file-name* option refers to the name of the file where the list of the IP addresses to be allowed or blocked is specified. The file must be in the **/var/db/url-filterd** directory and must have the same name as in the configuration.

  [See Integration of Juniper ATP Cloud and Web filtering on MX Routers .]

Software Defined Networking (SDN)

Software Installation and Upgrade

- **Migration of Linux kernel version**—Starting in Junos OS Release 21.4R1, the following devices support the Wind River LTS19 kernel version:

Platforms	Routing Engine Supported
ACX5448, ACX5448-D, and ACX5448-M	RE-ACX-5448

(Continued)

Platforms	Routing Engine Supported
MX240, MX480, and MX960	RE-S-X6
MX2020 and MX2010	REMX2K-X8
MX204	RE-S-1600x8
MX10003	RE-S-1600x8
MX2008	REMX2008-X8
MX10008, and MX10016	RE X10
PTX1000	RE-PTX1000
PTX5000	RE-PTX-X8
PTX10002	RE-PTX10002-60C
PTX10008	RE-PTX-2X00x4/RE X10
PTX10016	RE-PTX-2X00x4/RE X10
QFX10002	RE-QFX10002-60C
EX9204, EX9208, and EX9214	EX9200-RE2
EX9251	EX9251-RE
EX9253	EX9253-RE
SRX5400, SRX5600, and SRX5800	SRX5K-RE3 (SRX5k RE-2000x6)

Starting in Junos OS Release 21.4R1, in order to install VM Host image based on Linux WR LTS19, you have to upgrade the i40e NVM firmware to version 7.0 or later.

[See Upgrading the i40e NVM Firmware on Routing Engines with VM Host Support .]

Subscriber Management and Services

- **Support for subscriber service redundancy on DHCP server (MX Series)**—Starting in Junos OS Release 21.4R1, you can enable M:N subscriber service redundancy using active leasequery for the DHCP server running on an MX Series broadband network gateway (BNG). The subscriber service redundancy on the DHCP server ensures uninterrupted subscriber services when you reboot or replace the primary server, or when the primary server has any hardware failures such as access link failures, access line-card failure, or chassis failure.

  [See M:N Subscriber Service Redundancy on DHCP Server.]

- **Subscriber service reauthentication on actual data rate change (MX Series)**—Starting in Junos OS Release 21.4R1, the DHCP server reauthenticates the subscriber service when the actual data rate changes. This reauthentication is an alternative to RADIUS change of authorization (CoA) to change subscriber session characteristics based on the actual data rate change without interrupting the subscriber service.

  You can enable the reauthentication feature using the `actual-data-rate-change` statement at the `[edit system services dhcp-local-server reauthenticate]` hierarchy level. You can also configure a threshold value for the `actual-data-rate-change` downstream and upstream DSL attributes at the `[edit system services dhcp-local-server reauthenticate actual-data-rate-change]` hierarchy level.

  [See reauthenticate (DHCP Local Server), show subscribers, and show network-access aaa statistics re-authentication.]

- **Load-balancing support for subscriber traffic on pseudowire service interface (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.4R1, we support load balancing for subscriber sessions on the pseudowire service interface over multiple logical tunnel child member links of a redundant logical tunnel (RLT) interface at the same time. The load balancing property of the RLT interface allows subscriber traffic on the pseudowire service interface to be dispersed and load-balanced over different PICs and line cards. Service providers can enable BNG subscriber sessions on the PS interface with the support of multiple active links.

  An RLT interface allows up to a maximum of 32 member LT interfaces. This redundancy protects the access and the core-facing link against anchor Packet Forwarding Engine failure across line cards.

  [See Pseudowire Subscriber Logical Interfaces Overview.]

- **CoS support for BNG on pseudowire service interface over active-active RLT interface (MX240, MX480, and MX960)**—In Junos OS Release 21.4R1, we've introduced CoS support for a BNG on subscriber-interface on pseudowire over an active-active redundant logical tunnel (RLT) interface for subscriber applications such as DHCP and PPPoE. This CoS property is achieved by providing the scheduling nodes for the logical tunnel links. For dynamic interfaces, interface sets, static underlying interfaces, and dynamic underlying interfaces over RLT, CoS allocates scheduling nodes for each link in the RLT, which has multiple logical tunnel links in active-active mode. In case of targeted interfaces and targeted interface sets, which have primary and backup links, CoS allocates scheduling nodes on

the primary and backup links to optimize the use of scheduling nodes. Traffic for the subscriber targeted interfaces will be distributed to all the primary LT links when CoS is applied at the subscriber level.

When you enable targeting in a node, you must enable targeting for all the child nodes for CoS to function properly. Also, you must configure the network-services `enhanced-ip` at the `[edit chassis]` hierarchy level because this feature works only in enhanced IP mode.

[See Anchor Redundancy Pseudowire Subscriber Logical Interfaces Overview, targeted-options (PS interface), logical-interface-fpc-redundancy (PS interface), rebalance-subscriber-granularity, show interfaces demux0 (Demux Interfaces).]

VPNs

- **Antispoofing protection for next-hop-based dynamic tunnels (MX240, MX480, MX960, MX2010, and MX2020 with MPC10E or MX2K-MPC11E line cards)**—

  In Junos OS Release 21.4R1, we've added antispoofing capabilities IPv4 tunnels and IPv4 data traffic. Antispoofing for next-hop-based dynamic tunnels can detect and prevent a compromised virtual machine (inner source reverse path forwarding check) but does not apply to a compromised server that is label-spoofing. The antispoofing protection is effective when the VRF routing instance has label-switched interfaces (LSIs) using vrf-table-label or virtual tunnel (VT) interfaces. We do not support antispoofing protection for per-next-hop labels on VRF routing instances.

  [See Anti-Spoofing Protection for Next-Hop-Based Dynamic Tunnels Overview.https://www.juniper.net/documentation/us/en/software/junos/vpn-l3/topics/topic-map/l3-vpns-nh-tunnels.html#id-antispoofing-protection-for-nexthopbased-dynamic-tunnels-overview .]

- **Support for AMS in IPsec MX-SPC3 (MX240, MX480, and MX960 with MX-SPC3)** —Starting in Junos OS Release 21.4R1, the MPC10E (MPC10E-15C-MRATE and MPC10E-10C-MRATE) line card interoperates with the MX-SPC3 service card to support an aggregated multiservices interface (AMS).

  [See Aggregated Multiservices Interface.]

- **Support for AMS warm standby (MX240, MX480, and MX960 with MX-SPC3)**—Starting in Junos OS Release 21.4R1, the MPC10E (MPC10E-15C-MRATE and MPC10E-10C-MRATE) line card interoperates with the MX-SPC3 service card to support warm standby on an aggregated multiservices interface (AMS). In AMS warm standby mode, you can use a single service interface as a backup for multiple service interfaces.

  [See Aggregated Multiservices Interface.]

- **Support for headend termination of pseudowire services in a VPLS-enabled virtual switch (MX Series)**—Starting in Junos OS Release 21.4R1, you can configure a pseudowire service transport logical interface in Layer 2 circuit. You can also configure a trunk service logical interface in a VPLS-

enabled virtual switch to terminate a Layer 2 circuit instance in the virtual switch. You can terminate the same Layer 2 circuit in the VPLS instance-type routing instance with different service logical interfaces and Layer 3 VPN VRF instance-type routing instance using another service logical interface as well.

[See Pseudowire Service Interfaces.]

Additional Features

We've extended support for the following features to these platforms.

- **DHCP security** (EX9200, MX240, MX480, MX960, MX2010, MX2020). MPC10E line cards support the following DHCP security features:
  - DHCP snooping with Option 82.
  - DHCPv6 snooping with Option 16, Option 18, Option 37, and Option 79.
  - Lightweight DHCPv6 Relay Agent.

  [See DHCP Snooping.]

- **Dynamic routing protocols** (MX240, MX480, and MX960 with MX-SPC3, SRX5000 line of devices with SPC3 card and vSRX running iked). We support the exchange of dynamic routing information through IPsec VPN tunnels. You can now enable the dynamic routing protocol, such as OSPF, BGP, BFD, PIM, and RIP on a st0 interface of an IPsec VPN tunnel.

  This feature is supported only if the `junos-ike` package is installed in your device.

  [See Routing Protocols Support on IPsec VPN Tunnels.]

- **Enhancements to increase traffic selector flexibility** (MX240, MX480, and MX960 with MX-SPC3). You can do the following to add flexibility to your traffic selectors in different deployment scenarios:
  - Configure the routing metric for a traffic selector.
  - Define the source port range, destination port range, and protocol for a traffic selector.
  - Define multiple terms within a traffic selector, instead of creating multiple traffic selectors (or child security associations or SAs) for a VPN. Each term comprises the local and remote IP prefixes, the source and destination port ranges, and the protocol identifier. You can use these parameters in a single IPsec SA negotiation. In earlier Junos OS releases, you configure each traffic selector with one set of local and remote IP prefixes to be used in an IPsec SA negotiation with a peer.

  This feature is supported only if the `junos-ike` package is installed in your device.

We recommend that you configure the same metric value if you define multiple traffic selectors under the same `[edit security ipsec vpn vpn_name]` hierarchy with the same value for *remote-ip ip-address/netmask*. If you configure different metric values, then the metric value of the st0 route installed will be the same as that for the traffic selector that is negotiated or installed first.

[See traffic-selector and show security ipsec security-associations detail.]

- **EVPN Type 2 and Type 5 route coexistence** (EX9200, EX9251, EX9253, MX204, MX240, MX480, MX960, MX2010, MX10003, MX10008, and QFX10002-60C)

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

- **Hybrid mode (Synchronous Ethernet and Precision Time Protocol) over LAG supports PTP over IPv4 and PTP over Ethernet** (MX204 and MX10003)

  [See PTP Overview and Hybrid Mode Overview.]

- **Hold timer support on aggregated Ethernet (ae-) interfaces (MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, PTX1000, PTX5000, PTX10002, PTX10008, PTX10016)** Specify the hold-time value to delay the advertisement of up and down transitions (flapping) on an interface.

  [See hold-time.]

- **Redistribution of IPv4 routes with IPv6 Next Hop into BGP through tunnels: (MX10008 and MX10016):**

  IPv4 traffic is tunneled from CPE devices to IPv4-over-IPv6 gateways as described in RFC 5549.

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

- **Support for Precision Time Protocol (PTP) over Ethernet in hybrid mode over link aggregation group (LAG)** (MX10008 with JNP10K-LC2101 MPC line card)

  [See Precision Time Protocol Overview and Hybrid Mode Overview.]

- **Supported transceivers, optical interfaces, and DAC cables** (ACX Series, EX Series, PTX Series, MX Series, and QFX Series).—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

- What's Changed in Release 21.4R2 | 86
- What's Changed in Release 21.4R1 | 88

Learn about what changed in this release for MX Series routers.

What's Changed in Release 21.4R2

IN THIS SECTION

- General Routing | 86
- Layer 2 Ethernet Services | 87
- MPLS | 87
- Network Management and Monitoring | 87
- VPNs | 88

General Routing

- Stateful port configuration for PTP over Ethernet and default profile is supported only on boundary clock mode and not on ordinary clock mode.
- OpenConfig container names for Point-to-Multipoint per interface ingress and egress sensors are modified for consistency from **signalling** to **signaling**.
- **Router advertisement module status on backup Routing Engine (MX Series)**— The router advertisement module does not function in the backup Routing Engine as the Routing Engine does not send an acknowledgment message after receiving the packets. Starting in this Junos OS Release, you can view the router advertisement module information using the `show ipv6 router-advertisement` operational command.

  [See show ipv6 router-advertisement).]

Layer 2 Ethernet Services

- **New output fields for subscriber management statistics (MX Series)**—If you enable the enhanced subscriber management, the non-DHCPv4 bootstrap protocol (BOOTP) requests might not get processed even if you configure the DHCP relay or server with the `overrides bootp-support` statement at the `edit forwarding-options dhcp-relay` hierarchy level. To monitor the DHCP transmit and receive packet counters, we've introduced the following output fields for `show system subscriber-management statistics dhcp extensive` operational command. - BOOTP boot request packets received - BOOTP boot reply packets received - BOOTP boot request packets transmitted - BOOTP boot reply packets transmitted

  [See show system subscriber-management statistics.]

MPLS

- **Disable sending of RSVP hellos over a bypass LSP (MX Series)**— Junos routers send RSVP hello packets over a bypass LSP (when one is present), instead of the IGP next hop. To return to the original behavior specify the `no-node-hello-on-bypass` option.

  [See no-node-hello-on-bypass.]

Network Management and Monitoring

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

VPNs

- **Changes to `show mvpn c-multicast` and `show mvpn instance` outputs** —The FwdNh output field displays the multicast tunnel (mt) interface in the case of Protocol Independent Multicast (PIM) tunnels.

  [See show mvpn c-multicast.]

What's Changed in Release 21.4R1

IN THIS SECTION

- EVPN | 88
- General Routing | 88
- Interfaces and Chassis | 89
- Network Management and Monitoring | 89
- Routing Protocols | 89
- Subscriber Management and Services | 90

EVPN

- **Output for show Ethernet switching flood extensive**—The output for show ethernet-switching flood extensive now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as unilist. Previously, the output for show ethernet-switching flood extensive would misidentify the next-hop type as composite.

General Routing

- The range for source-pfe and destination-pfe at show class-of-service fabric statistics is now 0-15 (depending on platform type).

- **No support for PKI operational mode commands on the Junos Limited version (MX Series routers, PTX Series routers, and SRX Series devices)**—We do not support `request` , `show` , and `clear` PKI-related operational commands on the limited encryption Junos image ("Junos Limited"). If you try to execute PKI operational commands on a limited encryption Junos image, then an appropriate error message is displayed. The `pkid` process does not run on Junos Limited version image. Hence, the limited version does not support any PKI-related operation.

- **Renamed veriexec-check option**—We have changed the `veriexec-check` option of the `request system malware-scan` command to `integrity-check`. This update does not include any functional changes. You can

use the `integrity-check` option to check whether integrity mechanisms are enabled for the Juniper Malware Removal Tool.

[See request system malware-scan.]

Interfaces and Chassis

- When configuring multiple flexible tunnel interface (FTI) tunnels, the source and destination address pair needs to be unique only among the FTI tunnels of the same tunnel encapsulation type. Prior to this PR, the source and destination address pair had to be unique among all the FTI tunnels regardless of the tunnel encapsulation type.
- **Display the donor details of the IPv6 borrower interface**—The output for the `show interfaces` command now displays the donor details of the IPv6 borrower interface.

  [See show interfaces].

Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.

Routing Protocols

- The RPD_OSPF_LDP_SYNC message not logged?On all Junos OS and Junos OS Evolved devices, when an LDP session goes down there is a loss of synchronization between LDP and OSPF. After the loss of synchronization, when an interface has been in the holddown state for more than three minutes, the system log message with a warning level is sent. This message appears in both the messages file and the trace file. However, the system log message does not get logged if you explicitly configure the `hold-time` for `ldp-synchronization` at the **`edit protocols ospf area area id interface interface name`** hierarchy level less than three minutes. The message is printed after three minutes.
- To achieve consistency among resource paths, the resource path /mpls/signalling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter**ip-addr='address'**/state/counters**name='name'**/out-pkts/ is changed to /mpls/signaling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter**ip-addr='address'**/state/counters**name='name'**/. The leaf "out-pkts" is removed from the end of the path, and "signalling" is changed to "signaling" (with one "l").

Subscriber Management and Services

- **New output fields for subscriber management statistics (MX Series)**—If you enable the enhanced subscriber management, the non-DHCPv4 bootstrap protocol (BOOTP) requests might not get processed even if you configure the DHCP relay or server with the `overrides bootp-support` statement at the `edit forwarding-options dhcp-relay` hierarchy level. To monitor the DHCP transmit and receive packet counters, we've introduced the following output fields for `show system subscriber-management statistics dhcp extensive` operational command.

  - `BOOTP boot request packets received`
  - `BOOTP boot reply packets received`
  - `BOOTP boot request packets transmitted`
  - `BOOTP boot reply packets transmitted`

  [See show system subscriber-management statistics.]

Known Limitations

IN THIS SECTION

- Flow-Based and Packet-Based Processing | **91**
- General Routing | **91**
- EVPN | **92**
- Infrastructure | **93**
- MPLS | **93**
- Network Management and Monitoring | **93**
- Platform and Infrastructure | **93**
- Subscriber Access Management | **94**

Learn about known limitations in Junos OS Release 21.4R2 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.

Flow-Based and Packet-Based Processing

- Use 512 antireplay window size for an IPv4 or IPv6 in fat-tunnel. The ESP sequence check might otherwise report out-of-order packets if the fat-tunnel parallel encryption is within 384 packets (12 cores * 32 packets in one batch). Therefore, there are no out-of-order packets with 512 antireplay window size. PR1470637

General Routing

- When the device is up and running for a long time, there is a possibility FS gets bad blocks and it is accumulated. When any change done to it, it reloads and tries to recover the bad blocks from the FS. PR910445
- When cmerror disables the Packet Forwarding Engine, it does not power off the EA and HCM chips. Temperature monitoring continues on the HMC and other devices, and the system can take proper actions, such as increasing the fan speed or shutting down the systems. PR1324070
- On rebooting MPC11, errors such as following could be seen, but these are harmless and does not have functional impact. **timestamp device kernel: i2c i2c-100: (11/1:0x41) i2c transaction error (0x00000002) timestamp device kernel: i2c i2c-64: (7/1:0x41) i2c transaction error (0x00000002).** PR1457655
- IP options are not supported for egress firewall attach points. The issue might occur when IP-options router alert traffic is not hitting the egress firewall filter.

  [See IP-options router alert traffic not hitting the egress firewall filter .] PR1490967
- LFM might flap during MX Series Virtual Chassis unified ISSU to and from this release. PR1516744
- The issue applies to the initial release of CBNG for the Junos OS Release 22.1. Running `help apropos` command in configuration mode is generating an MGD core file. The MGD will comeback up and as long as the command is not issued again and the core will not occur. PR1552191
- The PTP FPGA is kept in reset during BIOS boot. During Linux boot, the PTP FPGA is taken out of reset and pcie-tree is reenumerated. Hence you would be seeing the Link-up/down during this sequence. PR1572061
- When a packet, which triggers ARP resolution, hits services interface style filter on the output will have session create and close log with incorrect ingress interface. This usually happens with the first session hitting such a filter. PR1597864

- On MX Series platforms, enhanced policer counter output shows double value when policer is applied in the ingress direction. The output shows normal when the filter is applied in the egress direction. PR1615373
- When the show command `show services web-filter secintel-policy-db ip-prefix-information` is being used, exact prefix mentioned in the feed file database needs to be provided. PR1615465
- When filter has next-term then it becomes unoptimized and started to get executed serially. Since all the terms are configured with the next term in the given configuration, forcing terms to be evaluated in the sequential manner instead of jump which causes the ppe thread to execute more than 900 instructions causing the bottleneck. PR1617385
- Percentage physical-interface policer is not working on the aggregated Ethernet interface, after switching between baseline configuration and policer configuration. PR1621998
- If we have scaled number of PPPoE subscribers hosted on PS anchored over RLT interface. Now, if we try to remove LT member link from the RLT bundle, then some of the subscribers might go down. So It is advised to bring down all the subscribers before removing RLT member links. PR1623641
- Media install (USB, PXE) and media-zeroize operations do not succeed and boot time is increased. PR1624053
- In ULC-based linecards, you can see duplicate leaf values for the following counters exported in /interfaces/interface/state/counters hierarchy. in-unicast-pkts in-broadcast-pkts in-multicast-pkts in-pause-pkts in-errors in-discards out-unicast-pkts out-multicast-pkts out-broadcast-pkts out-pause-pkts out-errors out-discards. These leaves are produced by picd and aftd-trio. PR1624864
- The available space check in case of: 1. Upgrade is 5 GB 2. Fresh Install is 120 GB. The scenario of upgrading or installing is decided from within RPM spec i.e. if RPM finds any older version is already installed. Since RPM-DB is destroyed during LTS-19 (vm-host) upgrade, rpm install scripts deduce the upgrade as fresh-install and look for 120GB free space. The warning can be ignored, as it has no functional impact. PR1639020
- The ZPL ISSU operation for MPC11E is incompatible to in-service-upgrade from releases to new releases with infra change in sysman_msg.emg PR1652737

EVPN

- EVPN-VXLAN ESI might result in minor loop in some scenarios and this might hit duplicate address detection (DAD) in IPv6. PR1619504

Infrastructure

- While upgrading the software image from Junos OS Release 21.2 to Junos OS Release 21.3, the `no-validate` configuration statement is mandatory for the upgrade command to proceed. PR1586481

MPLS

- With local reversion ON, there is a possibility of transit router not informing headend of RSVP disabled link when link flap more than once. Work around is to remove local-reversion configuration. PR1576979

Network Management and Monitoring

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

Platform and Infrastructure

- After clearing vpls mac table, the following error message occurs while running clear vpls mac-table. [Mar 9 06:20:42.795 LOG: Err] disp_force_callout(1994): EA[0:0].disp[0] forced callout timeout 0 msec. [Mar 9 06:20:42.795 LOG: Err] luss_send_callout_parcel(793): EA[0:0].disp[0] failed to send callout parcel (ptype 14, snum 977 tid 0). [Mar 9 06:20:43.510 LOG: Err] dispatch_event_handler(684): EA[0:0].disp[0] PRIMARY_TIMEOUT (PPE 4 Zone 8). There will not be any functional impact during this issue, just the error logs. It occurs with a scaled count of more than 1.5L MACs and eventually all the MACs will get cleared successfully. PR1575316

- When the `deactivate services rpm` and `deactivate routing-options rpm-tracking` CLIs are applied together and then committed, some of the rpm tracked added routes are not deleted from the routing table. Issue cannot be seen using the following steps. 1. deactivate routing-options rpm-tracking 2. commit the configuration then all the rpm tracked routes will be deleted. If the RPM service need to be deactivated, 3. deactivate services rpm 4. commit. PR1597190

- After a switchover event, when ppmd calls sendmsg system call to transmit the protocol packets, it gets blocked long enough that a few sendmsg calls cumulatively take up around 7 to 8 seconds. This indirectly impacts the BFD session because the BFD session has a Routing Engine-based detect time of 7.5 seconds to expire. PR1600684

Subscriber Access Management

- A restart of APM's provisioning micro-service (prov-man) when connected to a BNG or BNGs might result in the inability for APM to re-establish a functional APMi connection with a BNG or BNGs. This is a result of the BNG's inability to detect the loss of the initial connection. The BNG's JSD service has gRPC keep-alive settings which make connection loss detection difficult.PR1645910

Open Issues

IN THIS SECTION

- Class of Service (CoS) | **95**
- EVPN | **95**
- Forwarding and Sampling | **95**
- General Routing | **96**
- Interfaces and Chassis | **102**
- Juniper Extension Toolkit (JET) | **102**
- Layer 2 Ethernet Services | **103**
- Layer 2 Features | **103**
- MPLS | **103**
- Network Management and Monitoring | **104**
- Platform and Infrastructure | **104**
- Routing Protocols | **106**
- User Interface and Configuration | **106**
- VPNs | **106**

Learn about open issues in Junos OS Release 21.4R2 for MX Series routers.

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

Class of Service (CoS)

- In certain conditions, a stale rewrite rule entry is left behind in the Packet Forwarding Engine and the corresponding kernel state is incorrect. The pre-conditions to note this phenomenon include a sequence of aggregated Ethernet specific operations along with the present of CoS configuration.PR1649510
- The aggregated Ethernet interfaces in per-unit-scheduler mode and committing the CoS configuration on the aggregated Ethernet logical interfaces in a single commit leads to race-conditions.PR1656441

EVPN

- In Provider Backbone Bridging - Ethernet VPN (PBB-EVPN) environment, ARP suppression feature which is not supported by PBB might be enabled unexpectedly. Therefore, MAC addresses of remote CE devices are not learned resulting in traffic loss. PR1529940
- EVPN-MPLS multihoming control MACs are missing after removing VLAN ID and adding back on a trunk logical interface of one of the multihoming PE devices. This is not a recommended way to modify VLAN ID configuration. Always both multihoming PE devices need to be in symmetric. PR1596698
- EVPN local ESI MAC limit configuration is not effective when the remote multihoming MACs learn the MAC limit. As a workaround, clear the MAC table from all multihoming PE devices and configure the MAC limit over the local ESI interfaces. PR1619299

Forwarding and Sampling

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

General Routing

- If a vmhost snapshot is taken on an alternate disk and there is no further vmhost software image upgrade, the current vmhost image might corrupt and the system reboots with the alternate disk. The user can recover the primary disk to restore the state. However, the host root file system and the node boots with the previous vmhost software instead of the alternate disk. PR1281554
- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. PR1362609
- On MX Series routers with MPC7E, MPC8E, or MPC9E installed, if optics QSFPP-4X10GE-LR (part number 740-054050) is used, the link might flap. PR1436275
- When you boot MPC11 linecard, the following harmless errors are seen. These errors have no functional impact. timestamp device kernel: i2c i2c-100: (11/1:0x41) i2c transaction error (0x00000002) timestamp device kernel: i2c i2c-64: (7/1:0x41) i2c transaction error (0x00000002. PR1457655
- The following error might be seen on the MX Series routers with XQ chip (for example, MPC5E, MPC2E-3D-NG-Q, MPC3E-3D-NG-Q, and more.) or EA chip (for example, JNP10003-LC2103, MPC7E, and more). fpcx Cmerror Op Set: XQCHIP(46): XQ-chip[0]: SCHED L4NP[0] Parity errors (status=0x20000). PR1464297
- When hardware link errors occur on all 32 links on an FPC 11, all FPCs reports destination errors towards FPC 11. The FPC 11 is taken offline with "offlined due to unreachable destinations" reason. PR1483529
- When you run the `show pfe filter hw filter-name` *`filter name`* command, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. PR1495712
- When backup Routing Engine stops, CB1 goes offlbn; and comes back online. This restarts the backup Routing Engine, and it shows the reboot reason as "0x1:power cycle/failure".

  PR1497592
- In the platform using indirect next hop (INH), such as Unilist as route next hop type for multiple paths scenario (such as BGP PIC or ECMP), the session fast-reroute might be enabled in the Packet Forwarding Engine. When the version-id of session-id of INH is above 256, the Packet Forwarding Engine might not respond to session update because the session-id might stuck permanently with the weight of 65535 in the Packet Forwarding Engine. It might lead the Packet Forwarding Engine to have a different view of unilist against load-balance selectors. Then either the BGP PIC or the ECMP-FRR might not work properly and traffic might be dropped or silently discarded. PR1501817
- The JFlow service might not report accurate throughput rate. This issue is seen when there is high sampled traffic rate with low flow cache hit ratio.PR1502645

- A delay of 35 seconds is added to the reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 21.4R2. PR1514364
- In MAC-OS platforms when a client connects successfully, the client will not be minimized to tray icon and it stays connected and needs to manually minimize it. PR1525889
- Due to BRCM KBP issue route lookup might fail. As a workaround, you can upgrade KBP. PR1533513
- The Flexible PIC Concentrator (FPC) might generate a core file if the flap-trap-monitor feature under `set protocols oam ethernet cfm performance-monitoring sla-iterator-profiles` is used resulting in performance monitoring flap.PR1536417
- On a scaled MX2020 router with `vrf localisation` enabled, 4 million next hop scale, and 800K route scale, FPCs might go offline on GRES. Post GRES, router continues to report many fabric related CM_ALARMs. FPC might continue to reboot and might not come online. Rebooting master and backup Routing Engine will help recover and get the router back into a stable state. PR1539305
- The FPC process might not get spawned after hard reboot in a rare case, which causes the FPC to not come online successfully. PR1540107
- On MX480 router, the following error message appears: **Feb 27 20:26:40 xolo fpc3 Cannot scan phys_mem_size.out. Please collect /var/log/*.out (0;0xdd3f6ea0;-1) (posix_interface_get_ram_size_info): Unknown error: -1**. PR1548677
- Running `help apropos` command in configuration mode will generate an MGD core file. PR1552191
- The script compiles an unsupported configuration that hits the maximum threshold for the given platform. PR1555159
- 5M DAC connected between QFX10002-60C and MX2010 do not link up. But with 1M and 3M DAC, this interoperability works as expected. On QFX10002-60C and ACX or traffic generator the same 5M DAC works seamlessly. PR1555955
- VE and CE mesh groups are default mesh groups created for a given routing instance. On VLAN or bridge-domain add, flood tokens and routes are created for both VE and CE mesh-group or flood-group. Ideally, VE mesh-group does not require on a CE router where IGMP is enabled on CE interfaces. MX Series based CE boxes have unlimited capacity of tokens. PR1560588
- Due to a race condition, the `show multicast route extensive instance` *`instance-name`* output displays the session status as Invalid. Such an output is a cosmetic defect and not indicative of a functional issue. PR1562387
- Configure an interface hold time to avoid the additional interface flap. PR1562857
- Stale TCNH entries are seen in new primary Routing Engine after switchover with NSR even though all the prpd routes are deleted. These TCNH entries are present because NSR is not supported for

BGP static programmable routes. This leads to an extra reference count in the backup Routing Engine, because next hop is not free. PR1566666

- On MX Series platforms, when inline Jflow is configured at high sampling rate (more than 4000 per second) is set, high CPU utilization might be observed and this might result in relevant impacts on traffic analysis and billing. PR1569229
- In MX Series devices, the device might not send pause frames in case of congestion. PR1570217
- When aggregated Ethernet link is brought down, a transient error message, **[Error] Nexthop: EalNhHandler: failed to add Nh: xxxx, type: composite, as pil add failed** might be seen. There is no functional impact due to these errors. PR1570710
- A vulnerability in handling exceptional conditions in Juniper Networks, Junos OS Evolved (EVO) allows an attacker to send specially crafted packets to the device, causing the advanced forwarding toolkit manager (evo-aftmand-bt or evo-aftmand-zx) process to crash and restart, impacting all traffic going through the FPC, resulting in a Denial of Service (DoS). PR1572969
- The following messages might be seen in the logs from MPC11E line-card: Feb 9 11:35:27.357 router-re0-fpc8 aftd-trio[18040]: [Warn] AM : IPC handling - No handler found for type:27 subtype:9. There is no functional impact and these logs can be ignored. PR1573972
- In EVPN-VXLAN scenario with OSPF configured over the IRB, OSPF sessions might not get established because of the connectivity issues. PR1577183
- Path validation fails for network-instances protocols. PR1579439
- When you configure /8 pool with block size as 1 and commit, the block creation utilizes more memory causing NAT pool memory shortage which is currently being notified to customer with syslog tagged RT_NAT_POOL_MEMORY_SHORTAGE. PR1579627
- In a fully loaded device, the firewall programming fails at times due to scaled prefix configuration with more than 64,800 entries. However, this issue is not observed in development setup. PR1581767
- Under the conditions of the bridge domains in the virtual-switch type instance having "vlan-id-list", Bridge domain names information is not displayed properly in `show bridge statistics instance`. PR1584874
- When the active secondary interface is deactivated, the PTP lock status is set to 'INITIALIZING' state in `show ptp lock-status` output for few seconds before BMCA chooses the next secondary interface. This is the day-1 behavior and there is no functional impact. PR1585529
- In rare circumstances during GRES, the routing protocol daemon will restart generating a core file in the former active Routing Engine (new backup Routing Engine). PR1589432

- Inline NPT on MX Series routers does not translate the source IPv6 of packet with authentication header present. The packet is simply passed through upstream. Consequently, it is not expected that downstream traffic arrives with NPT pool IPv6 address as IPv6 destination address and with Authentication header. Such traffic might be malicious and this must be handled via external configuration. The fix suggested is to configure firewall for downstream direction that blocks traffic destined to NPT pool address and with authentication header. PR1592957
- Pim VxLAN does not work on TD3 chipsets enabling VxLAN flexflow after Junos OS Release 21.3R1. PR1597276
- On all MX Series routers, changing configuration AMS 1:1 warm-standby to load-balance or deterministic NAT might result in generating vmcore file and cause traffic loss. PR1597386
- On the MX10016 platform, PICs might not come online for all FPCs in case "spmb" process restarts immediately after the power cycle. PR1597630
- On MX Series routers, compact forwarding engine board (afeb) process might crash with MIC-3D-8DS3-E3. If a MIC-3D-8DS3-E3 having any hardware fault is initialized into the device. The AFEB crash will restore automatically in sometime and faulty hardware need to be replaced. The AFEB crash might impact the traffic forwarding during the time of issue. PR1598411
- Release note needed PR1600502
- It seems that ubuntu root-fs 18.04 shipped in the latest release does not have the "en_US.UTF-8" locale enabled by default. PR1601262
- When the interface transitions from down to up, the carrier transition counter value of a particular interface can be incorrect when the peer interface takes longer time to come up. PR1601946
- The convergence time degradation is seen in IS-ISv6, OSPFv2, and OSPFv3 when comparing convergence time with Junos OS Release 21.1R1.5. As it is a convergence time issue, many components are involved and hence need investigation of rpd, kernel, and Packet Forwarding Engine. PR1602334
- In vMX platform, after a system reboot, the protect-Routing Engine filter on lo0 interface is no longer applied. PR1604401
- Rebooting JDM from inside JDM shell changes JDM's main PID as a result systemd's knowledge of JDM PID becomes stale. Due to this reason systemd fails to stop or start JDM. PR1605060
- An RPD agent sends an INH deletion or additions out of order to backup RPD, RPD generates a core file. PR1607553
- IS-IS adjacency remain down in backup Routing Engine during MOFRR convergence test.PR1608591
-

When high pps traffic sent for a 'establish tunnels on-tarffic' IPsec VPN with S2S configuration, IKED process will be inundated with IKE trigger and IKE negotiation messages from peer. This causes a delay in handling messages at IKED process and timeouts for IKE negotiations, and eventually results in tunnels not getting established. This issue might occur when the tunnels are negotiated for the first time or when one of the VMS in the AMS bundle goes down. PR1610863

- Several warning messages show up while the RPD process restarts during performing GRES on a system running Junos EVO. PR1612487
- Changing aggregated Ethernet mode (aggregated-ether-options link-protection) with subscribers logged in on that aggregated Ethernet will cause undesirable subscriber management behavior. Users will need to confirm there are no subscribers on the aggregated Ethernet before changing the aggregated Ethernet protection mode. PR1614117
- In some NAPT44 and NAT64 scenarios, duplicate SESSION_CLOSE syslog will be seen. PR1614358
- Mastership switch is not supported during FRU reconnect during master release" is observed.PR1615344
- MPC gets rebooted while enabling FLT for inet6 filter with 10000 terms, instead of fallback to DMEM filter gracefully. Currently, fast lookup filter supports up to 8000 terms. PR1617174
- Fabric errors could be expected when SLC is restarted when ISSU is in progress, to avoid this problem "do not restart SLC when ISSU is in progress". PR1619180
- USF-SFW:Memory Zone is not reflecting properly while doing memory tests via Vty command test usp service-sets memory-testing start" . PR1619499
- Destination errors will be seen when unified ISSU is done on GNF without enhanced-mode. This is seen with and without SLC configuration. PR1620705
- System_id formate of AFT-MPC(MPC10E) is not aligned with non-AFT MPCs. PR1622073
- Fabric goes to check state the configurations when the SLC / GNF ISSU is in progress. PR1622511
- When installing an IPv6 firewall filter using BGP flowspec, matching traffic counters might show "0" values. PR1623170
- Cannot login to dhcp or pppoe client on double-tagged dynamic vlans. PR1623785
- in scaled setup with ldp over rsvp configuration and maximum-ecmp as 32 or 64, line card CPU usage can remain high for extended duration on link flap operation. In this duration, LACP can take more than 5 minutes to move from detached to CD state. PR1624219
- flowd core file is observed with TLB configuration only with combination of MPC10 card with older MPC card. PR1624572

- Pkid crashes due to null pointer dereferencing during local certificate verification in some cases. PR1624844
- DHCP v6 server binding will not happen, when mld-snooping is enabled along with DHCP v6 snooping. PR1627690
- For a topology with VSTP and VRRP configured and IPv6 traffic, if VSTP bridge priority is changed a couple of times (to trigger toggling of root bridge), it is possible that IPv6 traffic drop is seen on some of the streams. PR1629345
- On ACX5448, MX204 and MX2008 VM Host-based platforms, starting with Junos 21.4R1 or later, ssh and root login are required for copying line card image (chspmb.elf for MX2008) from Junos VM to Linux host during installation. The ssh and root login are required during installation. Use the deny-password instead of deny as default root-login option under ssh configuration to allow internal trusted communication. Alternatively, once installed, it can be disabled in the configurations. Refer to TSB18224. PR1629943
- Zeroize RPC returns no positive reply. PR1630167
- In scaled setup with high number of nexthops and routes, a configuration churn might lead to high CPU utilization and delayed convergence for Indus and Daniel MPC linecards. PR1631612
- DSLite do not work on MX Series platform installed with MPC7E line card and SPC3 service PIC. PR1632278
- It is noted that the single hop BFD session over aggregated Ethernet is not fully functional after exercising Packet Forwarding Engine reset feature. The BFD session was up before Packet Forwarding Engine reset operation is initiated but after the reset the BFD rx session is not fully functional. PR1632585
- During ZPL ISSU of MPC10 or MPC11 line cards, if LACP and LFM configurations are present, PPMAN core might be seen. PR1633286
- On MX Series routers with SPC3 service card installed, TFTP control sessions are getting refreshed with inactivity time-out after data session is closed, causing the control session to stay in session table for some more time. Service impact is minor or negligible as the TFTP control session will eventually get deleted after timeout. PR1633709
- FRR loss of around 18- 20 seconds is seen during LAG bundle failure triggers with scaled configuration. PR1636785
- WIth PTPoIPv6 on MPC2E 3D EQ, PTP secondary stays in acquiring state. PR1642890
- Under some circumstances, alarmd will generate core file due to some discrepancy in Junos-synchronization component. PR1643743

- Issue is specific to YT cards during mlp delete messages the logical interface ktree lookup is resulting in an incorrect dword for the IIF registry. Because of this counter address is incorrectly read resulting in ppe traps. Issue is not seen in ZT cards. PR1645483
- With overlapping NAT pool configured with different NAT rules under different service sets, when service outside interface is moved between different routing instances (for example, from vr1 to default, and from default to vr1), NAT routes corresponding to the service-set in default routing instance are getting deleted, resulting in reverse path traffic failure for NAT sessions. PR1646822
- Core file seen while testing "hcm_dpi_pcef_usf_3.robot". PR1648886
- Traffic drop might be observed on MX960 platforms for some MAC entries which are learned on interchassis control link (ICL) instead of multichassis link aggregation (MC-AE). PR1653926
- The low priority stream might be marked to destinate error. As a result, the low priority stream gets stuck and traffic drops. PR1657378

Interfaces and Chassis

- ICCP does not come up when mc-lag PE is rebooted since static ARP is deleted and never re-installed back. Therefore, it is not recommended to configure ICCP over IRB which is associated with mc-lag bridge 166 domain. Customer upgrading from old release to new release (PR 1075917 support) might come across issue like static ARP is not reinstalled for remote mc-lag IRB IP when existing static ARP entry is removed. PR1409508
- When family bridge is configured, logical interfaces are not created. If logical interfaces are not created, l2ald does not create IFBDs (interface to BD association) and if we do not have IFBDs in the system, STP is not enabled on that interface. PR1622024
- On all Junos OS platforms, the addition or removal of VRRP group might flap the other VRRP group under the same physical interface. The bug causes the already existing configuration of all VRRP groups under the same physical interfaces (along with the ones where no configuration change is being committed) to be treated as a new configuration and eventually deletes it before adding it back. Therefore, all VRRP sessions flaps and virtual-router uptime is reset. PR1658966

Juniper Extension Toolkit (JET)

- Abrupt termination of the client socket may take time for the disconnect to be detected by JSD. The client would have to wait for the connection terminal to be detected in such cases, which could be around 1 hour or restart JSD before being able to connect back with the same client ID. PR1549044

- The stub creation functions are present in *pb2_grpc.py. PR1580789
- GRPC on WAN port is not working. The libsi can only be linked with 64-bit binaries. To access data or WAN ports, you need to link libsi with the binary. By default, the shell on the device includes libsi, but it is not available to the CLI commands as the CLI will make mgd invoke cscript to run a Python script through CLI. PR1603437

Layer 2 Ethernet Services

- On MX5, MX10, MX40, MX80, and MX104 Series platforms with DHCP server configuration for DHCP subscribers, the jdhcpd memory leak might occur and the memory increase by 15MB depends on the number of subscribers when testing the DHCP subscribers log-in or log-out. PR1432162
- Making configuration changes with apply-group add/delete associated with DHCP might result in the client connection failure. PR1550628

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 20--50 ms traffic drop on the existing logical interface. PR1367488

MPLS

- BFD session flap during unified ISSU only in MPC7E card (BFD sessions from other cards of DUT to peer routers did not flap during unified ISSU). Issue is not seen frequently. PR1453705
- In MVPN case, if the nexthop index of a group is not same between primary and backup after a nsr switchover, you might see a packet loss of 250 to 400 ms. PR1561287
- The use-for-shortcut configuration statement is meant to be used only in SRTE tunnels which use SSPF (Strict SPF Algo 1) Prefix SIDs. If `set protocols isis traffic-engineering family inet-mpls shortcuts` and `set protocols isis traffic-engineering tunnel-source-protocol spring-te` is configured on a device, and if any SRTE tunnel using Algo 0 Prefix SIDs is configured with `use-for-shortcut` configuration statement. This might lead to generate routing loops or rpd core files. PR1578994

- LDP session authentication key-chain configuration based on session remote-id on initiator stops from session establishment even though the responder's authentication key-chain is configured for its remote-id. PR1592431
- On the MX10016 routers, when there is scaled RSVP sessions (for example, 21,000) and the RSVP is enabled for all the interfaces, then the rpd process goes through all the interfaces which results into a high CPU utilization for some time. This also results in LSP flap. PR1595853
- RPD crashes continuously in backup Routing Engine with below configuration `set routing-options static route destination-prefix p2mp-ldp-next-hop root-address p2mp-root-address lsp-id` *`lsp-id`* `set routing-options warm-standby`. PR1645457
- PPPOE_V4 traffic stream is not within threshold (+/-10%) range of 100mbps. Issue is seen after GRES and it can impact in traffic loss or PPPoE subscriber bringup failure. PR1649763
- On all Junos OS platforms, if `[edit routing-option resolution preserve-nexthop]` hierarchy is configured globally, Routing-engine (RE) kernel crash might be observed in the one-hop-LSP MPLS scenario with Routing Engine outbound traffic.PR1654798

Network Management and Monitoring

- Junos has a feature to block or deny all hidden commands. Users can get this feature by configuring `set system no-hidden-commands`. However, when this is configured and committed Junos OS blocks or denies new netconf or junoscript XML sessions. As a workaround, users can delete `system no-hidden-commands` configuration statement and start the new netconf or junoscript sessions. PR1590350
- A minor memory leak is seen in the event-daemon process when multiple GRES switchovers are performed. PR1602536
- mgd can crash when an invalid value is configured for identityref type leafs/leaf-lists while configuring Openconfig or any other third-party YANG, problem occurs with json and xml loads. PR1615773

Platform and Infrastructure

- The traps are the result of PPE commands injected from the host. One possible reason might be Layer 2 BD code, which is trying to decrement BD MAC count in the data plane. It is unlikely that there is a packet loss during this condition. This could happen during unified ISSU and this might be due to a problem with the unified ISSU counter morphing used for LU-based cards, where certain counters are not disabled or disabled too late during the unified ISSU. PR1426438

- With GRES and NSR functionality with VXLAN feature, the convergence time might be slightly higher than expected for L2-DOMAIN-TO-L3VXLAN. PR1520626
- When the DHCP relay mode is configured as no-snoop, the offer gets dropped due to incorrect ASIC programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. PR1530160
- During Routing Engine switchover, interface flap might be seen along with scheduler slippage. PR1541772
- When a EX4400 Virtual Chassis is scaled with different features configurations and device is stressed with traffic, device might not respond for CLI commands for a short period of time and a vmcore might be reported at that time. Once VM core is saved, device will continue to operate normally. PR1599498
- Do notuse the control-type light under platforms where this feature is not supported at present. At present IPv4 and IPv6 twamp-light is supported on the platforms using TRIO and PE chipsets. PR1603128
- Traffic loss of is observed with vrrp mastership change from backup to master. This is seen while we bring up the route back after enabling the link. PR1612504
- On MX Series platforms, during reboot, the aggregated Ethernet logical interfaces are first added, then deleted and again added. This flapping causes corner case where the filter attachment IPC has older aggregated Ethernet logical interface index on which the filter bind fails. Filter will not be attached to the interface, so any filter related service will not work. PR1614480
- Using static labeled switched path (LSP) configuration, the child node is not removed from the flood composite when the core interface goes down.PR1631217
- MACs are not getting learned initially on a specific bridge domain. However, the MACs are learned in that specific BD after some duration. This delay in MAC learning will be fixed in the upcoming releases. PR1632411
- The CLI configuration can be used to bump the ARP packets priority to use NC3 in case customers have continuous congestion of best-effot queue. `set system arp arp-request-bump-priority`. PR1644973
- When multihop multipath EBGP is configured over IPsec tunnels established using SPC3, vmcore files are seen. PR1646428
- In MX Series platforms, if a small size packet (for example 64 byte) is transmitted out of the queue, the Packet Forwarding Engine gets disabled.PR1657203

Routing Protocols

- TILFA backup path fails to install in LAN scenario and also breaks SR-MPLS tilfa for LAN with more than four end-x sids configured per interface. PR1512174
- Multicast traffic is hogging the switch core when `igmp-snooping` is removed. The MCSNOOPD will generate a core file due to the changes in mrouter interfaces and routes. PR1569436
- When MPLS traffic engineering and rib inet.3 protect core file is enabled then transport routes in inet.3 will not be used for route resolution. PR1605247
- On MX Series routers, initial multicast register packets might get dropped. This might affect the multicast services. PR1621358
- When filter is configured through an open config and bound to a Routing table instance, the filter bind object is not getting published due to the absence of Routing table object. Hence, the filter does not work as expected since the traffic does not hit the filter. PR1644421
- In all Junos OS platforms, when the BGP neighbor is brought down because of the prefix count received exceeds the prefix-limit configured. If BGP is disabled and then enabled, the BGP session might be brought up and then the rpd process crash might be observed.PR1655228
- On all Junos platforms, the rpd core file might be observed when the next hop for multicast upstream is not available. PR1658458

User Interface and Configuration

- File delete with regex might fail, if using filename without regex works. PR1624562

VPNs

- Tunnel debugging configuration is not synchronized to the backup node. It needs to be configured again after RG0 failover. PR1450393
- On all Junos OS platforms with MVPN scenario, stale PIM (S, G) state might be seen when there are no local/remote receivers and the multicast source is inactive. Only stale PIM entry will be seen, and it does nt impact MVPN service or functionalities. PR1536903
- In certain cases, the PUSH ACK message from the group member to the group key server might be lost. The group member can still send rekey requests for the TEK SAs before the hard lifetime expiry.

Only if the key server sends any new PUSH messages to the grooup members, those updates might not be received by the group member since the key server would have removed the member from registered members list. PR1608290

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.4R2 | **107**
- Resolved Issues: 21.4R1 | **120**

Learn about the issues fixed in this 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: 21.4R2

IN THIS SECTION

- Class of Service (CoS) | **108**
- EVPN | **108**
- Forwarding and Sampling | **109**
- General Routing | **109**
- High Availability (HA) and Resiliency | **115**
- Interfaces and Chassis | **115**
- J-Web | **115**
- Layer 2 Ethernet Services | **116**
- MPLS | **116**
- Network Management and Monitoring | **117**
- Platform and Infrastructure | **117**
- Routing Policy and Firewall Filters | **118**

- Routing Protocols | **118**
- Services Applications | **119**
- Subscriber Access Management | **119**
- User Interface and Configuration | **119**
- VPNs | **119**

Class of Service (CoS)

- Interface burst size becomes low in Packet Forwarding Engine, when `rate-limit-burst` statement is removed. PR1650089
- Hierarchical Class of Service (HCOS) might not work for LT interfaces configured on PIC 2 and PIC 3 of MPC5E and MPC6E. PR1651182

EVPN

- Baseline EVPN-VXLAN transition from IPv4 to IPv6 or vice verse does not work in certain sequence. PR1552498
- Bridge mac-table learning entries might not be as expected for the EVPN-MPLS routing instance. PR1600310
- Few ARP/ND/MAC entries for VLANs are missing with MAC-VRF configuration. PR1609322
- Traffic loss for profile TI2-Inter-VN-Traffic_Stream-SH-MH when testing EVPN with VxLAN. PR1628586
- The l2ald crash might be seen after restarting routing on EVPN PE device. PR1629426
- Removing configuration statement `es-label-oldstyle` does not take effect if it is the only statement configured under the EVPN protocol. PR1629953
- The rpd might crash when moving an interface from VPLS to EVPN-VPWS instance. PR1632364
- The traffic loss might be seen when the link goes down for the local ESI. PR1632723
- IRB might not send out arp-reply if `no-arp-suppression` is configured. PR1646010
- The DF and BDF both might be up or forwarding in EVPN multihoming single-active scenarios. PR1647734

Forwarding and Sampling

- The response for `clear interfaces statistics all` command with scale configuration is delayed. PR1605544
- Packet loss is observed after hitting the firewall filter on a Junos OS platform. PR1625309

General Routing

- Error message "sensord: Error updating RRD file: /var/run/sensord.rrd" might be seen on WRL9-based line card. PR1420927
- PTP packets drop depending on the multicast configuration. PR1442055
- The pkid process might be observed during local certificate enrollment. PR1573892
- "CHASSISD_FRU_IPC_WRITE_ERROR: fru_send_msg: FRU GNF 2, errno 40, Message too long" might appear periodically in the chassisd logs. PR1576173
- NAT EIM mapping will create even for out to in FTP ALG child sessions. PR1587849
- Implement FW reload option to MX10008 in the CLI. PR1594579
- The mspmand daemon memory leak might be observed after the HA master goes down. PR1598356
- EVPN-VXLAN: RE1 went to DB prompt when tried loading profile configurations over LRM configurations. PR1598814
- PTP stateful configuration along with ordinary clock mode do not work together. PR1601843
- Fix for `show system errors fru detail` not displaying `reset-pfe` as the cmerror configured action. PR1602726
- After rebooting the JDM from shell mode, you cannot stop the JDM again. PR1603637
- VRRP and BFD might flap on an IRB interface on MPC10 and MPC11 line cards. PR1604150
- Kernel error logs (tcp_timer_keep) is seen on backup Routing Engine when `set system internet-options no-tcp-reset drop-all-tcp` option is enabled. PR1605255
- In the AMS bundle traffic might not be load balanced across member interfaces on MX Series Virtual Chassis. PR1605284
- VM host platforms might boot exactly 30 minutes after executing `request vmhost halt` command. PR1605971
- 5G-CUPS:bbe-cups-5G-setup:wf-eabu-dev.tadcaster:re1 {version} vmcore.0.gz. PR1606146

- 'WO-0: OGE0 dequeue watermark hit' might be seen with L2 related configuration and receiving jumbo-frame packets.PR1606967
- IPv6 link-local BFD session might not come up on MX Series routers. PR1607077
- MX204: Interface flap might be observed on certain ports. PR1609988
- The PFE/SIB/SCBE/FPCs might reboot due to the unexpected fabric errors shown up on MX240/480/960 platforms. PR1612957
- MPC6E 3D did not come up after MIC offline online test. PR1614816
- The counter might show double value when chassis enhanced-policer is configured. PR1615373
- ICMP error packet does not have relevant header when configured with DSLite and with appropriate ICMP ALG name and one UDP application name. PR1616633
- The Strict-Priority-Scheduler (SPS) might not work accurately across port queues. PR1616772
- A device which is configured IP interface (ip-x/x/x) cannot sent out encapsulated IPv4-over-IPv6 packets to a remote device in case of transit packets. PR1618391
- DHCP subscribers might not synchronize to backup BNG when DHCP ALQ is configured without topology-discover. PR1620544
- DHCP ALQ needs a new configuration parameter to adjust failover times. PR1631770
- The jdhcpd daemon might crash after upgrading Junos OS. PR1649638
- Flapping of all ports in the same Packet Forwarding Engine might disable the Packet Forwarding Engine. PR1621286
- FPC might crash on MX10003 when MACsec interfaces configured with bounded-delay feature are deleted in bulk. PR1621868
- When PHY-sync state moved to false, it internally disables the PHY-timestamping of PTP packets. PR1622108
- High phase jump spikes approximately from 4000 ns to 5000 ns during secondary clock fail-over within the same line card on commiting the configuration. PR1622575
- Constant increase of PCS errors might be seen on the channelized port. PR1622741
- The mcontrol might frequently miss keepalives from the backup Routing Engine. PR1624623
- The aggregated Ethernet member link might not be correctly populated on the Packet Forwarding Engine after FPC restarts on the MX Series routers. PR1624772

- On single IPsec tunnel with PMI when sending internet traffic packet processing might get delayed due to session management issue. PR1624974
- The flowd process lost heartbeat for 45 consecutive seconds without raising an alarm. PR1625579
- The bbe-statsd crash might be seen in the LTS subscriber scenario. PR1625648
- gNMI set RPC might fail when multiple values within a single gNMI SetRequest are used for the Junos telemetry interface. PR1625806
- Fabric request timeouts and fabric healing occurs. PR1625820
- Packet loops in the PIC even after stopping the traffic on MX Series routers with SPC3 line card. PR1625888
- The bbe-smgd might crash on backup Routing Engine after unified ISSU or GRES. PR1626091
- Traffic drop might be seen in node slicing scenario. PR1626115
- Some Interfaces might not come online after the line card reboots. PR1626130
- [technology/inlineservices] [core] : mx960 :: spd core file is seen. PR1626311
- After configuring 4000 bridge domains messages log file is flooded with kernal messages. PR1626381
- The chassisd might crash on MX104. PR1626486
- The autoconf might not work if the DHCPv4 discover message has option 80 (rapid commit) ahead of option 82. PR1626558
- Broadcast traffic might not be forwarded to LT interface in VPLS routing instance after LT interface is deleted then added back. PR1626714
- VPLS MAC age time-out might not be applied on some MAC addresses. PR1627416
- The `show vlan` command might not show appropriate output in all the Junos platforms. PR1627558
- Subscribers might face connectivity issues because of the memory leak. PR1627562
- DHCP clients might not go to BOUND state when the aggregated Ethernet bundle is enabled between DHCP server and snooping device. PR1627611
- "agentd_telemetry_uninstall_sensor: Deleting subscription from daemon aftsysinfo failed after mgmt_sock_retries 601, ret -1" error message is seen after stopping jtimon. PR1627752
- Invalid IP length packets encapsulated within MPLS might trigger PPE traps. PR1628091

- Memory leak might occur on PFED process when the `flat-file-profile` is configured with the `use-fc-ingress-stats` statements. PR1628139
- EAPol packets over Layer 2 circuit might get dropped at the tunnel start. PR1628196
- Tunnel-service bandwidth should not be changed when there are active subscribers. PR1628628
- The "monitor traffic interface" might not work for em2 on vRR/JRR200. PR1629242
- `show system subscriber-management route summary` does not report route summary as expected. PR1629450
- MX10008 is going to offline state as chassis connection drops after a fresh USB installation. PR1629558
- The l2ald might be stuck in "issu state" when unified ISSU is aborted. PR1629678
- The egress traffic on non-targeted iflset of subscribers might not be forwarded correctly over targeted aggregated Ethernet interface. PR1629910
- Multiple link flaps and traffic might be lost on the links. PR1630006
- The kmd daemon might crash generating a core file every few minutes on MX Series platforms. PR1630070
- LACP timeout might be observed during high CPU utilization. PR1630201
- With SCBE3+SPC3, fabric drops are seen around 10M PPS/60G TCP traffic with approximately 750 byte packet size with IPv6 SFW on a single PIC PR1630223
- Index of the link might get missed in the distribution table of Packet Forwarding Engines after the flap. PR1630408
- LLDP packets might be sent with incorrect source MAC for RETH/LAG child members. PR1630886
- The FPC might crash after enabling MACsec. PR1631010
- A clksync crash might be observed and PTP might get stuck. PR1631261
- Precision Time Protocol (PTP) might not lock on the MX Series platforms with MX-MPC2E-3D-P and MPC2E-3D LC linecards. PR1631274
- The kmd might crash since the pkid requested memory leak occur on MX Series platforms. PR1631443
- IPv6 host route prefix match disappear from 'forwarding-table' after a ping test. The 'ping' continues to work, forwarding table entry is not shown. No impact is seen in traffic. PR1631607
- Operations dependent on the SDB shared memory might be impacted. PR1631858

- RPD core file on RE1 @ krt_inh.c,krt_nexthop.c,krt_remnant.c. PR1631871
- When deleting the VNI and there is another VLAN ID-list with a different VNI might cause a traffic loss. PR1632444
- The bbe-smgd process might crash after removing and adding a child link from aggregated Ethernet interface. PR1633392
- The linecard crash might be observed in a subscriber scenario. PR1633825
- Slow chassis memory leak might occur when chassisd related configuration change is committed. PR1634164
- In subscriber scenario, traffic drop might be seen when aggregated Ethernet member link is removed. PR1634371
- PTP clock class might incorrectly be downgraded to 248 when PTP is enabled on linecard/MIC which does not support phy-timestamping. PR1634569
- The FPC might crash on enabling port-mirroring. PR1634570
- LACP interface might go down when a sub-interface configuration is added and committed to the aggregated Ethernet interface. PR1634908
- When all configured anchor Packet Forwarding Engines are offline on the SAEGW-u, there may be a peer association mis-match between the SAEGW-u and SAEGW-c. PR1634966
- CFM CCM PDU is not forwarded transparently on core file MX if the physical interface is configured under protocols oam. PR1635293
- BCM SDK publish build fails with error message in description is fixed. PR1635318
- Data might not be exchanged via EVPN-VxLAN domain. PR1635347
- Precision Time Protocol (PTP) packets having huge correction-field (CF) value coming out from MX Series routers. PR1635877
- FPCs might restart because of the faulty PEM module. PR1636118
- SFP-1FE-FX might not function properly on MIC-MACSEC-20G. PR1636322
- Wrong interface statistics might be reported on MX204. PR1636654
- The interface equipped with a QSA adapter might go down. PR1636874
- FPC crash might be seen on all MX Series devices with BBE subscriber. PR1637304
- Delay might be observed for the interfaces to come up after reboot/transceiver replacement. PR1638045

- Locally switched traffic might be dropped on MX10003 with ESI configured. PR1638386
- PFE might get stuck after 100G/400G interface flaps. PR1638410
- CCL:NGPR: RPD_KRT_RESPOSE_ERROR: krt change failed for prefix error from kernel is "EINVAL -- Bad parameter in request. PR1638745
- MX10008 having less required planes for fabric bandwidth degradation behaviour. PR1639212
- Time difference is not as expected when DUT exports interface-queue-stats to ipfix-collector tool after changing reporting-interval. PR1639378
- pon TLVs from PPPoE-IA tags are not displayed in the `show subscribers extensive` when preference is set to 'dsl'. PR1640277
- "show ldp p2mp tunnel" might not display the correct information. PR1641412
- Traffic might be dropped due to the RX queue being full. PR1641793
- Traffic drop due to incorrect memory allocation for the default route on MPC10E and MPC11E line cards. PR1642851
- PFED CPU increased post ISSU and remains around 65-75 percent for 32000 L2VPN sBNG services. PR1643077
- ICMP TTL exceeded packets are not sent out of the switch. PR1643457
- The openconfig network-instance/protocols/static-routes/static id list-key might generate an error on encoding through NETCONF. PR1644319
- Type5 traffic drop for BGP prefix on Scapa as remote leaf. PR1644458
- Post autobandwidth make-before-break, on enabling traffic over conditional metric LSP might silently drop or get discarded. PR1643587
- Video console for vRR might not work after an upgrade. PR1644806
- Traffic drop with EBGP multipath and EBGP paths equal to the maximum-ecmp limit. PR1645296
- MX104 - `request chassis afeb restart` returns timeout error. PR1645322
- The eBGP session might not be established on MX Series devices with MS-MPC and MX-SPC3 cards. PR1645585
- Multicast upstream rpf session status is stuck in an unexpected init state. PR1647746
- Intermittent traffic drop due to lookup loop with ipv4_arp_ipv6_nd_process_check_arp_nd_pkt and lmem addr error with ppe trap and auto ttrace. PR1650854

- BGP PIC edge might drop or discard the traffic after selector corruption PR1653562
- When fib-streaming is enabled and two or more collectors are involved, the fibtd core file might be observed due to time synchronization issue. PR1653942

High Availability (HA) and Resiliency

- Unified ISSU is getting aborted with ISSU is not supported for Clock Synchronization (SyncE). PR1652838

Interfaces and Chassis

- ACX7509 :: One LAG would support 64 member links for 21.4R1-EVO PR1627951
- The subscribers might be deleted when `host-prefix-only` statement is configured on the underlying-interface in GRES scenario. PR1630229
- The syslog messages and the dcd crash might be seen in Junos OS. PR1633339
- VRRP route tracking for routes in VRF might not work if `chained-composite-next-hop ingress l3vpn` is used. PR1635351
- Some daemons might get stuck when snmpd is at 100 percent CPU utilization. PR1636093
- FPC might crash if the continuity-check interval under CFM is modified. PR1636226
- `show vrrp extensive` command do not show the next logical interface "Interface VRRP PDU statistics". PR1637735
- On Junos OS Release 20.3 and later, the tracking routes of VRRP might become unknown after upgradation. PR1639242
- Traffic loss might be seen for the MAC addresses learned on the ICL interface. PR1639713
- The aaggregated Ethernet interface with 400GE flaps on adding and then removing a 400GE member link. PR1641585
- The RCP session number reaches the maximum limit with an impact on the traffic. PR1643855
- The lacpd might not come up on one of the links in the aggregated Ethernet bundle. PR1647145
- Authenitcation key cannot be configured with more than 15 character. PR1650873

J-Web

- Significant performance improvements were made to JWeb in this release. PR1652676

Layer 2 Ethernet Services

- Circuit-id handled incorrectly with backup node for ALQ with topology discover configured. PR1620461
- The jdhcpd process crashes in DHCP/DHCPv6 environment. PR1625011
- Option 82 might not be attached on DHCP request packets. PR1625604
- IPv6 IA_NA or IA_PD routes might get deleted from the DHCPv6 client. PR1629171
- Non-DHCPv4 BOOTP protocol packets might not be processed if enhanced subscriber management is enabled. PR1629172
- Aggregated Ethernet interface remains up after deleting the loopback and ae interface IP on the neighbor while verifying BFD sessions on the router. PR1640240
- The jdhcpd core file might be seen if TCP connection is restarted between the ALQ peers. PR1644919

MPLS

- Standby secondary LSP might get stuck on the same path as primary LSP upon reoptimization. PR1615326
- LDP protections paths might not be established when `auto-targeted-session` statement is deactivated and activated again. PR1620262
- Unexpected traffic loss on LSP headend might be observed when downstream IGP metric changes. PR1625438
- The timestamp of 'MPLS traceroute detail' information does not calculate sub-second data properly. PR1632449
- VCCV BFD session keeps flapping between MX Series and peer device if ultimate-hop popping is enabled. PR1634632
- [mpls] [LDP-Tunneling] : mx2020 :: rpd core@ldp_destroy_lib is observed in MX2020 post GRESS. PR1635863
- The rpd memory leak might be observed in a subscriber management environment with RSVP. PR1637645
- LSP over broadcast segment stays down when RSVP setup protection is enabled. PR1638145
- Dynamic bypass LSP might flap at every re-optimization interval. PR1639292

- FRR and backup LSP is not triggered upon IGP change when RSVP graceful-restart or no-reliable is configured without global graceful-restart. PR1648833

Network Management and Monitoring

- Ephemeral instance configuration is not removed even after deleting the ephemeral instance from `set system` configuration database. PR1553469
- Rtsdbd core file might be seen when an IPsec configuration is activated and then deactivated. PR1610594

Platform and Infrastructure

- The ppmd process might crash after an upgrade on SRX Series platforms. PR1335526
- On MX Series and PTX Series platforms, vmcore on master Routing Engine might be reported because of the mbuf corruption. PR1602442
- MX Series-based line cards might crash when the Packet Forwarding Engine memory is hot-banking. PR1626041
- Unrealistic service accounting statistics might be reported because of the firewall counter corruption. PR1627908
- Error message "gencfg_cfg_msg_gen_handler drop" might be seen after performing the `commit` command. PR1629647
- The packet drop might be seen on an FPC on the MX Series devices. PR1631313
- IP monitor might install default route with incorrect preference value when multiple IP monitoring is configured PR1634129
- Continuous fabric link sanity check interrupts in intervals of weeks resulting in traffic drop at some point of fabric input block. PR1636060
- During unfied ISSU on MX Series platforms an FPC might crash. PR1637618
- vmxt_lnx core found @ topo_get_link jnh_features_get_jnh jnh_stream_attach. PR1638166
- The `input-vlan-map` (pop) might not work on PS interfaces if the native VLAN is in use on the uplink interface. PR1640254
- Routing Engine switchover might result in traffic loss in certain scenario. PR1643416
- SCB reset with Error : zfchip_scan line = 844 name = failed due to PIO errors. PR1648850

Routing Policy and Firewall Filters

- Existing routing policies might change when global default route-filter walkup is changed. PR1646603

Routing Protocols

- Observing commit error while configuring `routing-options rib inet6.0 static` on all Junos OS platforms. PR1599273
- The rpd might crash and restart when NSR is enabled. PR1620463
- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific BGP export policies. PR1626367
- Multipath route with List-NH which has Indirect-NH as members fails into BGP-LU. PR1626756
- eBGP multipath route get stuck in KRT queue. PR1626966
- For prefixes leaked from BGP to IS-IS, the P flag will be set for Prefix-SID advertised from IS-IS. PR1627322
- The traffic might be ceased in PIM scenario. PR1627990
- The contributing routes might not be advertised properly if `from aggregate-contributor` is used. PR1629437
- The multicast forwarding cache might not get updated after deactivating the scope-policy configuration. PR1630144
- The BGP ECMP might not work and multipath route wont be created PR1630220
- The rpd might crash when BGP labeled-unicast family routes are present and BGP multipath is turned on PR1630987
- The rpd might crash after clearing isis database PR1631738
- The rpd might get into an infinite loop while clearing IS-IS database. PR1632122
- The BGP session might flap after an rpd crashes with 'switchover-on-routing-crash' and NSR is enabled in a highly scaled environment. PR1632132
- IS-IS database might not be synchronized in some multiple areas. PR1633858
- Multipath route for a VPN prefix is formed due to incorrect BGP route selection logic. PR1635009
- The BFD session might be down when multiple addresses of the same subnet are configured. PR1635700

- The multicast traffic might get dropped in the Packet Forwarding Engine. PR1638141
- The BGP peer might stay down in shards after doing a rollback. PR1643246
- The BGP route might still be present in the multipath route after you increase the IGP cost. PR1643665
- Passive BGP session in no-forwarding instance might not come up. PR1645010
- BGP PIC protection is not working in virtual router. PR1653356

Services Applications

- L2TP tunnels go down and might not re-establish after restarting the bbe-smgd process. PR1629104
- Tunneled subscribers might get stuck in terminating state in L2TP subscriber scenario. PR1630150
- DTCP radius-flow-tap fails to program Packet Forwarding Engine when you trigger X-NAS-Port-Id exceeding 48 character length. PR1647179

Subscriber Access Management

- RADIUS Change of Authorization (COA) NAK might not be sent with the configured Source Address in a virtual-router environment PR1625858
- Event-timestamp in RADIUS Acct-Stop might show future time. PR1643316
- Pool drain with APM do not work. PR1652715
- JDI-RCT:BBE:Authd core@thr_kill () at thr_kill.S:3. PR1655832

User Interface and Configuration

- Junos upgrade might fail with error "configuration database size limit exceeded". PR1626721

VPNs

- You cannont install the multicast route after exporting the secondary routes from one instance to another. PR1562056
- The rpd process might crash during unified ISSU if the auto-sensing statement is enabled for l2circuit. PR1626219
- Type 7 routes might be lost in MVPN+PIM SSM scenario. PR1640487
- The multicast tunnel interface is not selected as per the draft-Rosen configuration. PR1642182

Resolved Issues: 21.4R1

IN THIS SECTION

- Application Layer Gateways (ALGs) | 120
- Class of Service (CoS) | 121
- EVPN | 121
- Forwarding and Sampling | 121
- General Routing | 122
- High Availability (HA) and Resiliency | 132
- Infrastructure | 132
- Interfaces and Chassis | 132
- J-Web | 133
- Junos Fusion Enterprise | 133
- Layer 2 Ethernet Services | 133
- MPLS | 133
- Multicast | 134
- Network Address Translation (NAT) | 134
- Network Management and Monitoring | 134
- Platform and Infrastructure | 134
- Routing Policy and Firewall Filters | 135
- Routing Protocols | 136
- Services Applications | 137
- Subscriber Access Management | 137
- Unified Threat Management (UTM) | 137
- User Interface and Configuration | 138
- VPNs | 138

Application Layer Gateways (ALGs)

- ALG traffic might be dropped. PR1598017

Class of Service (CoS)

- In a Junos Fusion deployment, dynamically removing and adding a logical interface under interface-set could lead to traffic control profile on the interface-set not working PR1593058
- Child mgd processes might get stuck when multiple sessions continuously ask for interface information PR1599024
- Traffic loss might be observed if per-unit-scheduler is configured on AE interface PR1599857
- 802.1p rewrite policies might not have any effect if the rewrite is tied to CCC interfaces PR1603909
- IEEE 802.1 rewrite rule might not work on MPC10 linecard PR1604943
- The fabric queues priority might not get changed after activate/deactivate CoS configuration PR1613541

EVPN

- Baseline EVPN-VXLAN transition from IPv4 to IPv6 or vice verse does not work in certain sequence. PR1552498
- The BUM traffic might be dropped after changing any configuration on the device without router-id. configured PR1576943
- Traffic loss might be seen under EVPN scenario when MAC-IP moves from one CE interface to another PR1591264
- Transit Traffic gets dropped post disabling one of the PE-CE link on a remote Multi-Home PE in EVPN-MPLS A-A setup with Dynamic-List NextHop configured PR1594326
- EVPN might not work properly in multi-homing setup PR1596723
- The device announces router-mac, target, and EVPN VXLAN community to BGP IPv4 NLRI. PR1600653
- Traffic loss for profile TI2-Inter-VN-Traffic_Stream-SH-MH is seen when testing evpn with vxlan. PR1628586
- Traffic loss ia seen for profile TI2-Inter-VN-Traffic_Stream-SH-MH when testing EVPN with VxLAN. PR1628586

Forwarding and Sampling

- Logical interface statistcs for as(aggregated sonet) are displayed double value then expected. PR1521223

- The snmpwalk might not poll the mib for dual-stack interface. PR1601761

General Routing

- On MX10003, despite of having all AC low/high PEM, "Mix of AC PEMs" alarm is raised PR1315577
- RE switchover does not work as expected while SSD failure occurs. PR1437745
- SSL-FP Logging for non SNI session PR1442391
- Inaccurate allocated memory for 'nh' and 'dfw_rulemask' under kernel might be observed PR1475478
- The following error messages are observed: unable to set line-side lane config (err 30) PR1492162
- New fan failure alarm that would be reported after 3 consecutive failure interrupt status is high. PR1500920
- With multi-services scaled config and Jvision monitoring running after routing-restart, protocols/ services remains down and rpd doesn't respond/recover PR1520977
- The BFD session status remains down at the non-anchor FPC even though BFD session is up after the anchor FPC reboots or panic. PR1523537
- CSPRNG is changed to the HMAC-DRBG and cannot be changed to either the FreeBSD Fortuna or the Juniper DYCE RNGs PR1529574
- cli show chassi picd fpc-slot pic-slot did not display qsfp modules firmware properly PR1533645
- The MACsec PICs may stay offline in the new primary after performing ISSU PR1534225
- Pfe statistics not shown GNF in sublc mode having PFE mapping from non-zero pfe PR1547890
- FPC crash may occur after flapping the multicast traffic PR1548972
- Some transmitting packets may get dropped due to the "disable-pfe" action is not invoked when the fabric self-ping failure is detected PR1558899
- The device may run out of service post GRES/ISSU PR1558958
- The MX150 device might reboot after performing `request system snapshot recovery` command. PR1565138
- Na-grpcd process can core during longevity tests PR1565255
- CLI-command "show pfe statistics traffic" shows wrong output PR1566065
- Junos OS and Junos OS Evolved: Local Privilege Escalation and Denial of Service PR1568654

- When using log templates (introduced in 21.1R1) with Unified Policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile (set security log profile name default-profile) that can be used to improve this behaviour when multiple log profiles are defined. PR1570105
- High CPU usage may occur on rpd for routes that use static subscriber PR1572130
- The fxpc process might crash and cause traffic loss in the IFBD scenario PR1572305
- DCPFE/FPC crash may be observed on the QFX10000 series platforms if ARP MAC move happens PR1572876
- Only root user is allowed to execute commands on host using vhclient. PR1574240
- DS-Lite throughput degradation might be seen on MS-MPC PR1574321
- MIC specific alarms are not cleared after MIC reboot PR1576370
- MPC7E, MPC10E, MX-SPC3 and LC2103 line cards might become offline when the device is running on FIPS mode PR1576577
- Mirrored packets are corrupted when port-mirror and discard actions are both applied. PR1576914
- MPC7E/8E/9E/11E line card might be stuck in "Unresponsive" state in a Junos Node Slicing setup PR1580168
- The static MACs configured over AE might not get programmed in forwarding after the FPC restart PR1581325
- Certain fields in the GNMI extension header and show network-agent statistics cli will have incorrect values if the input subscription path contains a ":" character PR1581659
- Junos OS and Junos OS Evolved: A vulnerability in the Juniper Agile License Client may allow an attacker to perform Remote Code Execution (RCE) (CVE-2021-31354) PR1582419
- Traffic drop might be observed on MX platforms with SPC3 in the DS-LITE scenario PR1582447
- Load balancing is not working correctly on AMS interfaces for CGNAT traffic on MX USF mode with SPC3 PR1582764
- The bcmd process might crash on the MX150 platform PR1583281
- Firewall filter is not getting programmed after deleting a large filter and adding a new one in a single commit on QFX5000 line of switches. PR1583440
- The Layer 2 multicast VXLAN instance goes down since local vtep logical child interface is not associated to the EVPN instance. PR1584109

- The secure web proxy continues to send the DNS query for the unresolved DNS entry even after removing the entry. PR1585542
- Packet loss might be seen during global repair of FRR. PR1586122
- `show security idp counters` do not have tenant statement in it's syntax. PR1586220
- The RPD_KRT_KERNEL_BAD_ROUTE error message is seen in certain scenarios when the rpd process restarts or GRES happens when NSR is enabled. This error has no functional impact.PR1586466
- Remove SIB without turning offline first might impact traffic. PR1586820
- The MVPN traffic loss might be seen due to the flooded multicast next-hop is missed PR1587054
- Junos Telemetry Interface leaves such as "used-power" and "allocated-power" under /components do not reflect correct value. PR1587184
- PEM capacity shows incorrectly on MX10003 platform. PR1587694
- Incorrect error message is observed when `request chassis cb slot 1 offline` statement is executed before node goes offline. PR1589433
- The aftd process might crash in firewall filter scenario. PR1589619
- Fabric link training could be seen if the fabric selfping silently gets discarded. PR1590054
- The `open configuration BGP route community` command output is incorrect when you use large BGP communities. PR1590083
- PTP synchronization might get unstable. PR1591667
- The mobiled daemon might crash after switchover for an AMS interface or crashes on the service PIC with the AMS member interfaces. PR1592345
- AMS warm standby with deterministic NAT functionality might not work properly. PR1592437
- Routing Engine kernel might crash because the logical interface of aggregated interface fails in the Junos kernel. PR1592456
- The duplicate Junos Telemetry Interface leaf of oper-status tag for logical interface index 16386 have mismatch value.PR1592468
- The L2cpd-agent might go unresponsive after starting telemetry service. PR1592473
- Using the BITS interface from backup RE for clock recovery might not work. PR1592657

- After Routing Engine switchover, the following error messages are seen:

```
JexprSlowCntrRead - Unable to get the plct Inst for pfeIdx: 255, User-type:
OVFM_OFFCHIP_NEXTHOP_CNTR.
```

  PR1593079

- The TCP connections to the telemetry server might be stuck in "CLOSE_WAIT" status. PR1593113
- On a Junos Node sliced setup if an SLC on MPC11E is restarted on some instances the interfaces on other SLC might also go down. PR1593500
- IPv6 neighbor might remain unreachable in VRRP for IPv6 scenario. PR1593539
- Jweb Deny log nested-application displays unknown instead of the specific application. PR1593560
- The dcpfe process might crash in an EVPN-VxLAN scenario. PR1593950
- PICD restart or crash might result in junks statistics for carrier transition. PR1594253
- The next-hop used for lawful intercept might not get installed correctly on the Packet Forwarding Engine of MPC10E or MPC11E line card which does not host the tunnel interface used for flow-tap service. PR1594380
- The BFD session for MPLS LSP goes down after enabling ultimate-hop-popping. PR1594621
- The label field for the EVPN Type 1 route is set to 1. PR1594981
- Inconsistent component name for FPC CPU is observed. PR1595109
- Application error alarms and trace-writer core files are generated due to defunct rcp zombie. PR1595409
- Layer 2 VPN stops forwarding when interface encapsulation is changed to vlan-ccc from ethernet-ccc and back. PR1595455
- Some TCP sessions might not be established after performing the `request system snapshot` command. PR1595470
- The interface down might be delayed after you issue the `set interface interface name disable` command. PR1595682
- Firmware might fail to be downloaded to MIC on the MX Virtual Chassis setup. PR1595693
- Mismatch in the master and backup Routing Engines with inetcolour tables and BGP-SRTE tunnels occur after rpd-restart on the primary Routing Engine. PR1596095

- Packet Forwarding Engine wedge might occur if many IPv4 packets are received that need to be fragmented. PR1596100
- The DCI InterVNI and IntraVNI traffic might silently be dropped and discarded in a gateway node due to the tagged underlay interfaces. PR1596462
- Mcscnoopd might crash when deleting and then adding layer-2 forwarding configuration after performing unified ISSU. PR1596483
- The nsd process generates a core file when you verify the session-limit rate and issue the `bypass-traffic-on-exceeding-flow-limits` command. PR1596578
- Traffic loss might occur periodically in the MACsec-used setup if the Routing Engine works under a pressure situation. PR1596755
- SR-TE tunnel initiated from a non-juniper PCE might fail PR1596821
- bbesmgd core generated after RE goes down. PR1596848
- Traffic fails to recover after multiple quick dot1xd restarts when you enable the MACsec suspend-for option. PR1596854
- The interface might not learn `mac-address` if it is configured with `vlan-id-list` starting with `VLAN id 1` and `native-vlan-id`. PR1597013
- Major alarms on all FPCs in chassis might be seen after some time from bootup. PR1597066
- The MAC/IP withdraw route might be suppressed by rpd in the EVPN-VxLAN scenario. PR1597391
- On MX10016 router, the SFB Plane not online alarm gets generated after the primary Routing Engine switchovers. PR1597630
- Major host 13 Ethernet interface link goes down with false alarm after RE1 is manually replaced. PR1597763
- MPC10E log messages will be observed with 'Temp Sensor Fail' alarm set/clear and 'cmtfpc_cpu_core_temp_get: Fail to get temp CPU7_PMB' messages. PR1597798
- The cfmman process might crash on MPC10 linecard running on FPCs. PR1597812
- Deletion of MACsec configuration on a logical interface does not take effect. PR1597848
- Inconsistency in the platform name used in multiple places, version, snmp mibs, and so on. PR1597999
- [subscriber_services][MX480] :: subinfo core file is generated with L2 node scaling. PR1598187
- Primary-only IP address keeps in old primary (new backup) and device becomes inaccessible after Routing Engine switchover. PR1598173

- arpd and ndp daemon crashes in scale setups. PR1598217
- Subscriber management daemons might continuously generate a core file and shutdown with Routing Engine sensor invalid configuration. PR1598351
- On MX10016 routers with JNP10K-RE1, unknown SMART attributes for StorFly VSFBM8CC200G SSD occurs.PR1598566
- Upper backplane type for the MX2020 router are incorrectly reported as Chassis. PR1598594
- The packet loop might occur after you receive the PCP request packets, which are destined to softwire concentrator address. PR1598720
- Component sensor does not export logs. PR1598816
- The l2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable. PR1599094
- False fan failure alarm flaps (set and cleared) frequently. PR1599183
- NSR switchover performed with BGP SR-TE tunnels might generate an rpd core file. PR1599446
- On MX SPC3 services card, ICMP protocol is not detected and does not allow user to modify inactivity-timeout values. PR1599603
- gNMI Telemetry might stop working after Routing Engine switchover. PR1600412
- The multiservices card does not drop the TCP acknowledgment packet received as a reply to the self-generated TCP keepalive. PR1600619
- The `config interface ip remove` command is not working appropriately. PR1600932
- Duplicate address detection (DAD) flags appear for the IRB interfaces after removing the configuration and restoring which might lead to traffic block. PR1601065
- Traffic loss might be seen on MPC10E and MPC11E under EVPN scenario. PR1601177
- The BBE-SMGD process generates core files at bbe_dequeue_and_deliver bbe_process_work_queues bbe_smd_main_post_dispatch. PR1601203
- Unable to commit configuration due to the Check-out failed error message for the mobility process. PR1601785
- Traffic might be dropped at NAT gateway if you enable EIM. PR1601890
- Kernel crash might be seen when static routes are configured with GRE interfaces being used as next-hop. PR1601996

- The IPv6 traffic might be impacted on the QFX Series or PTX Series platforms when an IPv6 route resolves over a dynamic tunnel. PR1602007
- A few line cards might not come up online with increased-bandwidth mode. PR1602080
- Under certain scaling scenarios, with EVPN-VXLAN configurations, l2ald might abort and recover. PR1602244
- After upgrading, configured firewall filters might be applied on incorrect interfaces (CVE-2021-31382). PR1602292
- Traffic might be lost when rewrite rules are configured on an aggregated Ethernet egress interface of MX Series platforms with MPC10E linecards. PR1602307
- Jflow-syslog for CGNAT might use 0x0000 in IPv4 identification field for all fragments. PR1602528
- The `show system errors fru detail` command is not displaying "reset-pfe" as the cmerror configured action. PR1602726
- The Packet Forwarding Engine might get disabled by a detected major CMERROR event when you ungracefully remove the MIC from MPC2E-3D-NG/MPC3E-3D-NG. PR1602939
- Junos OS: When using J-Web with HTTP an attacker might retrieve encryption keys via Person-in-the-Middle attacks. (CVE-2021-31386). PR1603199
- Packet loss might be seen on filter-based GRE deployments. PR1603453
- 21.3TOT:TCP_TLS_SYSLOG:core-usf-qnc-a-fpc3.pic1-flowd_spc3.elf.0.tgz is seeing while verifying TCP based logging functionality with GRES with AMS-Nexthop style PR1603466
- NSSU performed with MACsec configuration might generate fxpc core file. PR1603602
- The adapted sample rate might get reset to the configured sample rate without changing the sampling rate information in sFlow datagrams after configuring a new logical interface and enabling sFlow technology on this new logical interface at the same time. PR1604283
- NPC logs are observed when vrf localisation is enabled. PR1604304
- The following error message is observed: evo-aftmand-bt[18089]: [Error] IfStats:map entry not present for ifl:1039. PR1604334
- Interface hold-time up does not work on vMX and MX150 platforms. PR1604554
- The channel 0 physical interface does not come up after adding the correct speed configuration. PR1604810
- The interface on MCP3-NG HQoS/MPC7E flaps continuously after enabling LACP on aggregated Ethernet

interface. PR1605446

- The MPLS transit router might push an extra Entropy label to the LSP. PR1605865
- Multicast streams might stop flooding in VXLAN setup. PR1606256
- Segment Routing License issue might occur by default `chained-composite-next-hop` configuration. PR1606377
- Observing continuous SNMP trap for "Over Temperature!" for all the MX10016 line cards (FPC: JNP10K-LC480). PR1606555
- With dslite prefix-based subscriber and PCP the APP mapping for multiple PCP requests with suggested external ports is not behaving as expected. PR1606687
- New subscribers might not connect due to the CR-features service object missing on FPC. PR1607056
- TCP traffic might be dropped on source port range 512 to 767 when the FlowSpec IPv6 filter is configured. PR1607185
- In subscriber management scenario, under a rare condition, the Routing Engine reboots and generates a vmcore. PR1607282
- When l2ald restart, the following error message might be present, "L2ALIPC : L2AL IPC client is not connected to l2ald on restart l2-learning" PR1607580
- On MX Series platforms, error messages might be seen on triggering restart routing when sensors are configured. PR1608120
- Traffic load balance issue might be seen while toggling link-protection mode of RLT interface on-the-fly. PR1608300
- Address error case in open message to comply to RFC 8664 in PCCD and PCE_Server. PR1608511
- Memory leak might be observed on the l2cpd process when performing certain LLDP operations. PR1608300
- On PTX10K EVO platforms, defunct rcp processes increase which might cause master Routing Engine reboot. PR1608776
- High priority queue might not get the expected bandwidth on the EVO platforms. PR1609823
- The single-vlan tagged subscribers might fail to reconnect through dynamic-vlan over PS interface. PR1609844
- The authd process and RADIUS might have stale L2BSA subscriber entries. PR1610476

- "No filter found" error might be seen while deactivating the filter attached to the interface after MPC reboot. PR1616067
- After picd restart interface is down in channelized 100G link. PR1611379
- The service PICs are unable to come up when dnsf package is configured. PR1612316
- The Routing protocol engine CPU is getting stuck at 100 percent. PR1612387
- The B4 client traffic will be dropped on MX-SPC3 based AFTR in DS-Lite with EIM activated CGNAT scenario. PR1612555
- Some of the fabric links might go into faulty state after swapping FPC LC1201 with LC1202. PR1612624
- l2ald core file is generated during routing-instance configuration change. PR1612738
- Memory might be exhausted when both BGP rib-sharding and BGP Optimal Route Reflection (ORR) are enabled. PR1613104
- Traffic loss might occur due to the shaping rate being adjusted incorrectly in a subscriber environment on MX Series routers. PR1613126
- IGP routing updates might be delayed to program in Packet Forwarding Engine after interface flaps in a scaled BGP route environment. PR1613160
- For PS Service logical interface configured in MPC2-NG/MPC3-NG interface statistics do not show correct (shaped) value when shaping is applied. PR1613395
- IPsec tunnels are not deleted on disabling the AMS physical interface. PR1613432
- Enabling security-metadata-streaming DNS policy might cause a dataplane memory leak. PR1613489
- The rpd process might crash in BGP rib-sharding scenario. PR1613723
- Modifying the input-service-filter via COA might fail in subscriber management environment. PR1614903
- Line cards might be unstable due to the continuous growing memory usage of evo-cda-bt app. PR1614952
- Export memory and temperature metrics for all existing components when it subscribes to telemetry sensor. PR1615045
- The l2ald process might crash in EVPN scenario. PR1615269
- Request to provide an API which gives list of potential policy given a session id. PR1615355

- `show subscribers accounting-statistics`, `show services l2tp session interface asi0.xx statistics` might not work on LNS with asi- interfaces. PR1616454
- The dual Routing Engine system might not be GRES ready after backup Routing Engine reboot in a subscriber management environment. PR1616611
- Inconsistent error counts in `show interfaces brief` and `show interfaces extensive`. PR1616765
- In MXVC spcd running on SPC3 crashes. PR1617280
- MPC8E in 1.6T bandwidth mode might not work correctly. PR1617469
- Automatic Routing Engine switchover might not happen after migration. PR1617720
- Traceroute packets might get dropped in SFW service-set when other service-sets with asymmetric traffic processing are also enabled on the same MS-MIC/MS-MPC. PR1617830
- The traffic loss of CGNAT might be seen after cleaning the large-scaled CGNAT sessions in MS-SPC3 based Inter-Chassis High Availability scenario. PR1618360
- [macsec] [fips] Lowest acceptable PN do not reflect correct value when replay-window-size is more than zero. PR1618598
- The clksyncd might crash and PTP/SyncE might not work. PR1618929
- The nsd might crash while validating NAT translation on MX Series platforms with SPC3. PR1619216
- /interfaces/interface/subinterfaces/subinterface/state/counters are not exported during initial synchronization for on-change. PR1620160
- EVPN type 5 routes might not be installed. PR1620808
- All ports from the same Packet Forwarding Engine goes down at the same time causes mqchip_disable_ostream timeout then triggers host loopback path wedge and disable-pfe. PR1621286
- Invocation of `netconf get` command will fail if there are no L2 interfaces in the system. PR1622496
- Port speed might show as 100G even though chassis configuration is set for 40G manually. PR1623237
- The aggregated Ethernet member link might not be correctly populated on the Packet Forwarding Engine after FPC restart on MX Series platforms. PR1624772
- Implement `show task scheduler-slip-history` to display number of scheduler slips and last 64 slip details. PR1626148
- S-PTX10K-144C License SKUs do not load, 400G SKUs do load. PR1627459

- Evpn flood filter is not working for MPC10. PR1628270
- Commit related to dynamic profile configuration changes might fail upon executing "request vmhost reboot routing-engine both" on MX platforms PR1607494
- Adding and removing VLANs might cause traffic loss. PR1632444

High Availability (HA) and Resiliency

- When MTU is configured on an interface a rare ifstate timing issue might occur at a later point resulting in ksyncd process crash on backup Routing Engine. PR1606779

Infrastructure

- In tcpdump command processing allows an attacker to bypass configured access protections and execute arbitrary shell commands (CVE-2021-31357). PR1596122
- Upgrade might fail when upgrading from legacy release. PR1602005
- The fxpc process might crash and generate core file. PR1611480

Interfaces and Chassis

- Traffic might be interrupted while adding xe-/ge- interfaces as member of aggregated Ethernet interface bundle. PR1569399
- ARP resolution failure might occur during VRRP failover. PR1578126
- Junos Telemetry Interface optics sensor's alarm data type changed from " bool_val" to "str_val". PR1580113
- The dcd process might crash after performing Routing Engine switchover/reboot/management interface configuration change. PR1587552
- The dcd process crash might be observed after removing aggregated Ethernet logical interface from the targeted distribution database. PR1591032
- SIB might get stuck at an "offlining" state after performing offline and online operations. PR1591076
- Duplicate source and destination pair check is done only across same tunnel encapsulation type for FTI. PR1599266
- The dcd process might crash and FPC might be stuck in ready state on MX Series platforms. PR1601566
- The aggregated Ethernet interface might flap upon configuration changes. PR1602656

- LACP system priority might take a value of 0 and cause an LACP interoperability issue . PR1602724
- Few links on channelized interface is down after oir_enable and oir_disable in 4X25G. PR1606644
- Memory leak on dcd process occurs when committing configuration changes on any interfaces in a setup with AMS interface configured. PR1608281
- [interface] [platformtag] mx960 : :: PDT - MX960 : seeing dcd[40867]: %DAEMON-5: lo0 family maximum labels is non-adjustable in syslog messages. PR1611098

J-Web

- J-Web allows a locally authenticated attacker to escalate their privileges to root. (CVE-2021-31372) PR1594516

Junos Fusion Enterprise

- Reverting mastership from RE1 to RE0 might lead to l2ald daemon crash and cause an outage. PR1601817

Layer 2 Ethernet Services

- The traffic received on a port in LACP detached state might be incorrectly forwarded. PR1582459
- The DHCP client might be offline for about 120 seconds after sending the DHCPINFORM message. PR1587982
- Delegated prefix IPv6 address is missing in accounting stop messages. PR1588813
- The DHCP ALQ queue might get stuck causing subscriber flap. PR1590421
- Uneven traffic distribution might be observed between member links of LAG. PR1599029
- The rpd scheduler might continuously slip after GRES when there are 7000 DHCP clients in a subscriber management environment. PR1625617

MPLS

- The rpd process might crash in corouted bidirectional RSVP LSP scenario. PR1544890
- [mpls][generic] D-CSPF node segment label: unresolved when Node Index 0 configured. PR1564169
- The rpd core file is seen in the backup Routing Engine with in mirror_process_recvd_data_queue with mldp NSR configuration. PR1594405

- The LDP replication session might not get synchronized when dual-transport is enabled. PR1598174
- Sometimes MPLS LSP might go down due to a timing issue when a protected link goes down. PR1598207
- Static LDP P2MP might fail after NSR switchover. PR1598344
- The rpd might crash with LSP external controller configuration. PR1601763
- VPLS connection might get down if `dual-transport` is configured. PR1601854
- RSVP detour LSP might fail to come up when an LSR in the detour path goes down. PR1603613
- LDP P2MP traffic might be interrupted post GRES. PR1609559
- The rpd process might crash on standby_re LDP module when `vpls mac-flush` is enabled on peer by default or configuration. PR1610638
- Configuring protocols `mpls lsp-external-controller` also throws commit error if `in-place-lsp-bandwidth-update` is configured under any LSP. PR1612269
- The rpd process might crash if express segments using SR-TE underlay are configured. PR1613372

Multicast

- Intermittent p2mp traffic drop might be seen in MVPN scenario. PR1608311

Network Address Translation (NAT)

- Services NAT mappings and sessions are incorrect while checking the SIP sessions from public to private and RTP from private to public. PR1577922

Network Management and Monitoring

- The syslog archival transfer might fail if the archive site URL is configured with an IPv6 address. PR1603342
- SNMP reflects outdated ARP entries. PR1606600

Platform and Infrastructure

- The L2TP tunnel might not work with filter-based encapsulation. PR1568324
- Aggregated Ethernet interface queue statistics will be exported to Junos Telemetry Interface server. PR1571985

- FPC crashes on MX Series and EX9200 platforms. PR1579182
- The system generates an audit core file while changing TACACS and login user passwords. PR1589953
- Upon receipt of specific sequences of genuine packets destined to the device, the kernel will crash and restart (vmcore) (CVE-2021-0283, CVE-2021-0284). PR1595649
- VLAN tagged traffic might be dropped with service provider style configuration. PR1598251
- The service filter might get programmed incorrectly in Packet Forwarding Engine because of the rare timing issue in enhanced subscriber management environment. PR1598830
- There might be FPC core file and packet drop in VxLAN-EVPN scenario. PR1600030
- The mgd process might crash with an authentication setup. PR1600615
- The kernel core file might be seen if BGP connections are restarting after deleting BGP authentication. PR1601492
- The ZTP service might not work and the image installation fails. PR1603227
- RTT output might not get displayed when `show services rpm twamp client history-results` command is issued. PR1605243
- The FPC might crash if `flow-table-size` is configured on MX Series platforms. PR1606731
- Multicast traffic is dropped when forwarded over VPLS via IRB. PR1607311
- FPC crash might be seen because of mac-move between two interfaces under same bridge domain. PR1607767
- Degraded traffic processing performance might be observed in case of processing very high PPS rate traffic. PR1619111
- CoS custom classifier might not work on logical interface. PR1619630
- Configuration commit might fail while configuring `authentication-key-chains` statement under groups. PR1626400

Routing Policy and Firewall Filters

- BGP import policy is not applied to all the routes when CCNH inet is enabled. PR1596436
- The configuration check might fail if more than 8 FCs are configured and CBF is enabled. PR1600544
- The firewalld might crash if you configure `fragment-offset` statement outside the range (fragment-offset 1-900000000000). PR1605805

Routing Protocols

- BGP session might be down due to BGP-LS TLV received out of order. PR1546416
- Conformance issues with draft-ietf-idr-bgp-ext-opt-param. PR1554639
- Incorrect authentication-algorithm is set in BGP neighbor. PR1571705
- Short multicast packets drop using PIM when multicast traffic is received at a non-RPT/SPT interface. PR1579452
- Traffic drop might occur on link flap when IS-IS is configured. PR1585471
- The rpd crash might be seen if BGP peer flaps. PR1592123
- NTF-AGENT core file is seen at_**Tthr_rwlock_unlock CRYPTO_THREAD_unlock OPENSSL_init_crypto**. PR1597714
- After first parallel ISSU aborts, subsequent ISSU attempts on failed node aborts with 'Aborting Daemon Prepare'. PR1598786
- IPv4 static route might still forward traffic unexpectedly even when the static route configuration has already been deleted. PR1599084
- Some routes might get incorrectly programmed in the forwarding table in the kernel with next-hop installed as DEAD. PR1601163
- The rpd process might be stuck at 100 percent in OSPFv3 scenario. PR1601187
- Packet drop might be seen when changing INET MTU for MPLS enabled interface in IS-IS SPRING scenario. PR1605376
- MPC10E at [topgun] rpd core file `rt_table_flash_job_cancel`, `rt_instance_set_lsi_ifl_data_shard`, and `rt_flash_all_internal` might be seen after deactivating and then re-activating the interfaces. PR1605620
- IS-IS LSP might not be originated if `egress protection` is configured. PR1605969
- The BGP replication might be stuck in "InProgress" state. PR1606420
- Multicast traffic might be duplicated on subscriber interface on MX Series platforms. PR1607493
- With `rib-sharding` enabled any commit will flap all BGP sessions with 4 byte peer-as (AS number 65536 or greater). PR1607777
- `commit` might fail when `microloop-avoidance post-convergence-path` is configured with out SR and SRv6. PR1608992

- The rpd might crash after a commit if there are more than one address in the same address ranges configured under [bgp allow]. PR1611070
- The rpd crash might be seen on all Junos OS and Junos OS Evolved platforms. PR1613384
- Verification of BGP peer count fails, after deleting BGP neighbors. PR1618103
- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific bgp export policies. PR1626367

Services Applications

- `show services l2tp tunnel extensive`, `show services l2tp session extensive` and `show subscribers accounting-statistics` commands do not work on LTS. PR1596972
- Kmd core file has been generated at kmd_gen_fill_sa_pair_sadb_flags @kmd_update_sa_in_kernel @kmd_sa_cfg_children_sa_free. PR1600750
- `show services l2tp tunnel extensive`, `show services l2tp session extensive` commands provide incorrect outputs on LTS. PR1601886

Subscriber Access Management

- Subscribers might be stuck in terminated state when the RADIUS server is unreachable. PR1600655
- The "Service session entry creation failed" errors are seen during ephemeral commit. PR1603030
- Install discard routes is not supported on APM managed BNGs running Junos OS Release 21.3R1. PR1604967
- Prefix duplication errors might occur for DHCPv6 over PPPoE subscribers. PR1609403
- DHCP session fails with CLI `session-limit-per-username` statement. PR1612196
- BNG does not correctly issue abatement alarm to APM when condition is met. PR1626632
- When connectivity between BNG and APM is lost, the BNG does not regenerate pool drained alarms to APM. PR1627974

Unified Threat Management (UTM)

- There is no counter for juniper-local default action. PR1570500

User Interface and Configuration

- Updates to the system login configuration might not be reflected after a commit. PR1589858
- File copy command is not accepting HTTPS URIs. PR1596881
- The dfwc and dcd processes might crash when a `commit-check` is performed after a previously terminated (with ctrl+c) commit-check PR1600435
- The commitd core file may be observed after committing some configuration change. PR1601159
- Configuration transfer-on-commit not working if commit is done via netconf. PR1602331
- Invalid JSON and xml output format for command like `show system resource-monitor ifd-cos-queue-mapping fpc x | display [json|xml]`. PR1605897

VPNs

- The iked process might crash when IKEv2 negotiation fails on MX Series devices. PR1577484
- Cannot add BGP standard community to NGMVPN Type-6 and Type-7 routes in VRF export policy. PR1589057
- The rpd process might crash if the interface goes down in the BGP-MVPN scenario. PR1597387
- Wrong st0 IFL deletion at spoke when multiple VPNs negotiate same destination address as TS. PR1601047

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 documentation for MX Series routers.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

Basic Procedure for Upgrading to Release 21.4R2 | 139

- Procedure to Upgrade to FreeBSD 12.x-Based Junos OS | **140**
- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of- Life Releases | **143**
- Upgrading a Router with Redundant Routing Engines | **143**
- Downgrading from Release 21.4R2 | **144**

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

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

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

Platform	FreeBSD 6.x-based Junos OS	FreeBSD 12.x-based Junos OS
MX240, MX480, MX960, MX2010, MX2020	NO	YES

Basic Procedure for Upgrading to Release 21.4R2

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

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

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the juniper.conf and ssh files might be removed. To

preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see the Installation and Upgrade Guide.

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

Procedure to Upgrade to FreeBSD 12.x-Based Junos OS

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

To download and install FreeBSD 12.x-based Junos OS:

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

   https://www.juniper.net/support/downloads/

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

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

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-21.4R2.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-21.4R2.9-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-x86-32-21.4R2.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-21.4R2.9-limited.tgz
```

Replace source with one of the following values:

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

Do not use the `validate` option while upgrading from Junos OS (FreeBSD 6.x, 10.x, and 11.x) to Junos OS (FreeBSD 12.x). This is because programs in the **junos-upgrade-x** package are built based on FreeBSD 12.x, and Junos OS (FreeBSD 6.x, 10.x, and 11.x) would not be able to run these programs. You must run the `no-validate` option. The `no-validate` statement disables the validation procedure and allows you to use an import policy instead.

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

Rebooting occurs only if the upgrade is successful.

NOTE:

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.
- Starting in Junos OS Release 21.4R2, in order to install a VM host image based on Wind River Linux 9, you must upgrade the i40e NVM firmware on the following MX Series routers:
  - MX240, MX480, MX960, MX2010, MX2020, MX2008, MX10016, and MX10008

  [See https://kb.juniper.net/TSB17603.]
- Starting in Junos OS Release 21.4R1 and later releases, `ssh root-login` is required for copying the line card image (chspmb.elf) from Junos OS VM to Linux host during installation for MX204 and MX2008 VM host based platforms. Do not disable it through configuration during installation. Use `deny-password` instead of `deny` as default root-login option under `ssh` configuration to allow internal trusted communication.

  For information on VMHost based platforms, see VM Host Overview (Junos OS).

NOTE: After you install a Junos OS Release 21.4R2 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.

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 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

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

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

Upgrading a Router with Redundant Routing Engines

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

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

For the detailed procedure, see the Installation and Upgrade Guide.

Downgrading from Release 21.4R2

To downgrade from Release 21.4R2 to another supported release, follow the procedure for upgrading, but replace the 21.4R2 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for NFX Series

IN THIS SECTION

- What's New | **145**
- What's Changed | **146**
- Known Limitations | **146**
- Open Issues | **146**
- Resolved Issues | **148**
- Documentation Updates | **150**
- Migration, Upgrade, and Downgrade Instructions | **150**

These release notes accompany Junos OS Release 21.4R2 for the NFX Series Network Services Platforms. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

- What's New in 21.4R2 | 145
- What's New in 21.4R1 | 145

Learn about new features introduced in these releases for NFX Series devices.

What's New in 21.4R2

IN THIS SECTION

- Virtualized Network Functions (VNFs) | 145

Learn about new features introduced in this release for NFX Series devices.

Virtualized Network Functions (VNFs)

- **Support for virtual Router Reflector (vRR) VNF (NFX250 NextGen)**—Starting in Junos OS Release 21.4R2, you can implement the vRR capability on NFX250 NextGen devices by deploying a vRR VNF. Note that the vRR VNF is not supported on SR-IOV interfaces.

What's New in 21.4R1

IN THIS SECTION

- Network Management and Monitoring | 146

Learn about new features introduced in this release for NFX Series devices.

Network Management and Monitoring

- **Support for libvirt MIB (NFX150, NFX250 NextGen, and NFX350)**—Starting in Junos OS Release 21.4R1, you can monitor the performance of virtual machines by using the libvirt MIB. You can use either SNMPv2c or SNMPv3 to access the MIB data.

  [See Configuring SNMP on NFX150, NFX250 NextGen, and NFX350 Devices.]

What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R2 and 21.4R1 for NFX Series devices.

Known Limitations

There are no known limitations in hardware and software in Junos OS Release 21.4R2 for NFX Series devices.

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

Open Issues

IN THIS SECTION

- General Routing | **147**
- High Availability | **147**
- Interfaces | **147**

Learn about open issues in Junos OS Release 21.4R2 for NFX Series devices.

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

General Routing

- On the NFX350, if you change the device operational mode to custom mode, `ovs-vswitchd` cores might be seen on the device. PR1634245
- At times, L3 interfaces on the NFX150 device do not receive traffic when the SRIOV mapping changes from L2 interface to L3 interface. PR1612643
- On an NFX250 NextGen device, if you delete a vRR VNF and then add it back, the `show virtual-network-functions` command might show the vRR liveliness state as down.

  Workaround: Configure `dhcp force-discover` on the `em0` interface of the vRR VNF. PR1648041

High Availability

- On an NFX350 chassis cluster, when FPC0 (when node0 is primary) or FPC7 (when node1 is primary) is restarted by either using the `request chassis fpc slot slot restart node local` command or due to dcpfe core files on the primary, it restarts FPC1 or FPC8. This might break the preexisting TCP sessions and fail to restart the TCP sessions. The TCP sessions might require a manual restart. PR1557607

Interfaces

- (Applies to an NFX350 device with MACsec on the layer 2 interfaces) After you reboot an NFX350 device or restart the Packet Forwarding Engines on the device, the MACsec connectivity is not established on some of the links.

  WorkaroundDelete the layer 2 interface configuration for the affected links and then reconfigure it. PR1640451
- On the NFX250, the LACP subsystem does not start automatically when the dc-pfe process is restarted.

  WorkaroundDeactivate and then activate the aggregated Ethernet interface. PR1583054

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.4R2 | **148**
- Resolved Issues: 21.4R1 | **149**

Learn about the issues fixed in this release 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: 21.4R2

IN THIS SECTION

- General Routing | **148**
- Virtual Network Functions (VNFs) | **148**

General Routing

- On NFX150 devices, the destination service lookup does not work with UDP and TCP if a port range is not configured. PR1636174

Virtual Network Functions (VNFs)

- On all the NFX devices that have a VNF interface configured with trust mode enabled, VRRP is not functional.

  To resolve this issue, you must disable the spoof-check, using the CLI `set virtual-network-functions` *`vnf-name`* `interfaces` *`interface-name`* `mapping interface virtual-function disable-spoof-check`. PR1643164

Resolved Issues: 21.4R1

IN THIS SECTION

- Intrusion Detection and Prevention (IDP) | 149
- Interfaces | 149
- Platform and Infrastructure | 149
- Virtual Network Functions (VNFs) | 149

Intrusion Detection and Prevention (IDP)

- IDP predefined-attack-groups "Enterprise - Recommended" policy load fails on NFX250 NextGen devices due to insufficient heap memory on the data plane. PR1588881

Interfaces

- Unable to configure destination-port on firewall filter on NFX250 NextGen devices.PR1592019
- On NFX Series devices, deletion of VNF interfaces that are mapped SR-IOV interface fails. PR1598993
- L3 dataplane interfaces are not appearing when flex mode is enabled on NFX350-S3 devices. PR1599643

Platform and Infrastructure

- When the available free physical memory drops below 1.5 GB, configuration commits by Junos Device Management Daemon (JDMD) might not take effect and mustd core files are seen. This issue does not have any impact on the running traffic. PR1599641

Virtual Network Functions (VNFs)

- On NFX Series devices, while configuring vmhost vlans using vlan-id-list, the system allows duplicate VLAN IDs in the VLAN ID list. PR1438907

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for NFX Series devices.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | **150**
- Basic Procedure for Upgrading to Release 21.4R2 | **151**

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

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

NOTE: For information about NFX product compatibility, see NFX Product Compatibility.

Upgrade and Downgrade Support Policy for Junos OS Releases 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.

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 21.4R2

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

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

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

To download and install Junos OS Release 21.4R2:

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

   https://www.juniper.net/support/downloads/

2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the **Software** tab.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list to the right of the Download Software page.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.

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

Junos OS Release Notes for PTX Series

IN THIS SECTION

- What's New | 152
- What's Changed | 157
- Known Limitations | 161
- Open Issues | 161
- Resolved Issues | 163
- Documentation Updates | 169
- Migration, Upgrade, and Downgrade Instructions | 170

These release notes accompany Junos OS Release 21.4R2 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

- What's New in 21.4R2 | 153
- What's New in 21.4R1 | 153

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

What's New in 21.4R2

There are no new features or enhancements to existing features in Junos OS Release 21.4R2 for the PTX Series.

What's New in 21.4R1

IN THIS SECTION

- Hardware | **153**
- Class of Service | **153**
- MPLS | **154**
- Routing Protocols | **154**
- Services Applications | **155**
- Software Installation and Upgrade | **155**
- Additional Features | **157**

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

Hardware

Class of Service

- **Support for ToS/DSCP rewrite option protocol (PTX and QFX)**—Starting in Junos OS Release 21.4R1, you can mark IP ToS bits when IP packets enter MPLS tunnel during MPLS push events, by enabling the CoS rewrite feature 'protocol mpls' in your PTX Series and QFX Series devices. By enabling this configuration, you ensure that dedicated Internet access (DIA) traffic is not treated with QoS across the core of the network.
- [See Routing Policies, Firewall Filters, and Traffic Policers]
- **Support for CoS in EVPN-VXLAN topology (QFX5210)**—Starting in Junos OS Release 21.4R1, you can configure CoS on a QFX5210 L3 VXLAN gateway in an EVPN-VXLAN fabric. However, this configuration presents a few limitations:

- For uniform packet classification within the system, both the access port and the loopback port must have the same behavior aggregate (BA) or fixed classifier.
- If traffic from multiple access port converges on the same loopback port and if some of the access-port traffic needs a different classification, then you must apply a multifield classifier on the loopback port for the traffic of interest.
- PFC (both IEEE and DSCP based) is not supported as PFC backpressure will not reach the access port from network port due to the loopback port design.
- If you need a classifier on the network port (DSCP), you must have the same classifier on the network, loopback, and access ports, as network-to-access traffic also goes through the same loopback port.
- Other general VxLAN CoS limitations applicable for all QFX5000 switches apply to the QFX5210.

[See Understanding CoS on OVSDB-Managed VXLAN Interfaces and CoS Support on EVPN VXLANs]

MPLS

- **Support for new statement `no-normalize-same-members` to resize member LSPs (MX Series and PTX Series)**—In Junos OS Release 21.4R1, we've added the `no-normalize-same-members` statement to the container LSP normalization configuration under the `[edit protocols mpls container-label-switched-path NAME splitting-merging]` hierarchy. When you enable the `no-normalize-same-members` configuration, you only resize the existing member LSPs with equal bandwidth. In earlier Junos OS releases, if normalization does not need to create or delete any member LSPs, you resignal the member LSPs with equal bandwidth.

  [See splitting-merging.]

Routing Protocols

- **Higher DDoS bandwidth for Layer 2 and Layer 3 protocols (PTX1000, PTX10002, PTX10008, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, we support higher distributed denial-of-service (DDoS) bandwidth for many Layer 2 and Layer 3 protocols.

  [See protocols (DDoS) (ACX Series, PTX Series, and QFX Series).]

- **OSPF link delay measurement and advertising (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.4R1, you can measure and advertise various performance metrics in IP networks with scalability through probe messages that are sent by Two-Way Active Measurement Protocol (TWAMP) Light. OSPF receives probe messages and the measured values from TWAMP

Light. OSPF advertises these messages as TLVs in packets. You can use these metrics to make path-selection decisions based on the network performance.

[See How to Enable Link Delay Measurement and Advertising in OSPF.]

- **Enhanced support to handle `S` flag, `D` flag and `A` flags in IS-IS (MX Series and PTX Series)**—Starting in Junos OS Release 21.4R1, you can set the `S` flag to allow the label binding type, length and values (TLV) to leak through the IS-IS level (Level 1 or Level 2). You can set the `A` flag to program the penultimate-hop popping (PHP). You can set the `D` flag to prevent the leaking of the label binding TLV from Level 2 back to Level 1. Use the `no-binding` configuration statement at the `[edit protocols isis source-packet-routing no-binding-sid-leaking]` hierarchy level to disable label binding TLV leaks.

  [See Handling of the IS-IS Binding SID 'S' Flag and RFC 7794 Prefix Attribute Flags.]

- **Support for FAD and FAPM on traffic engineering database and BGP-LS (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.4R1, we support FlexAlgo Definition (FAD) and FlexAlgo Prefix Metric (FAPM) on the traffic engineering database and BGP Link State (BGP-LS). You can store FAD and FAPM entries in the traffic engineering database and BGP-LS. You can also store multiple prefix segment identifiers (SIDs) for a prefix in BGP-LS. You can import the FAD and FAPM entries from the traffic engineering database to BGP-LS and export the FAD entries from BGP-LS to the traffic engineering database.

  [See What is Flexible Algorithm Definition (FAD).]

Services Applications

- **IPv6 link-local address support for TWAMP Light (MX Series, vMX, PTX1000, PTX3000, and PTX5000)**—Starting in Junos OS Release 21.4R1, you can specify IPv6 link-local addresses for target addresses. You can also configure IPv6 addresses for source addresses that correspond to target addresses configured with IPv6 link-local addresses. To configure a TWAMP Light target address as an IPv6 link-local address, include both the:

  - `local-link` *`logical-interface-name`* option for the `target-address` statement at the `[edit services rpm twamp client control-connection` *`connection-name`* `test-session` *`session-name`*`]` hierarchy level

  - `control-type light` statement at the `[edit services rpm twamp client control-connection` *`connection-name`*`]` hierarchy level

  [See Configure TWAMP.]

Software Installation and Upgrade

- **Migration of Linux kernel version**—Starting in Junos OS Release 21.4R1, the following devices support the Wind River LTS19 kernel version:

Platforms	Routing Engine Supported
ACX5448, ACX5448-D, and ACX5448-M	RE-ACX-5448
MX240, MX480, and MX960	RE-S-X6
MX2020 and MX2010	REMX2K-X8
MX204	RE-S-1600x8
MX10003	RE-S-1600x8
MX2008	REMX2008-X8
MX10008, and MX10016	RE X10
PTX1000	RE-PTX1000
PTX5000	RE-PTX-X8
PTX10002	RE-PTX10002-60C
PTX10008	RE-PTX-2X00x4/RE X10
PTX10016	RE-PTX-2X00x4/RE X10
QFX10002	RE-QFX10002-60C
EX9204, EX9208, and EX9214	EX9200-RE2
EX9251	EX9251-RE
EX9253	EX9253-RE
SRX5400, SRX5600, and SRX5800	SRX5K-RE3 (SRX5k RE-2000x6)

Starting in Junos OS Release 21.4R1, in order to install VM Host image based on Linux WR LTS19, you have to upgrade the i40e NVM firmware to version 7.0 or later.

[See Upgrading the i40e NVM Firmware on Routing Engines with VM Host Support .]

Additional Features

We've extended support for the following features to these platforms.

- **Hold timer support on aggregated Ethernet (ae-) interfaces (MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, PTX1000, PTX5000, PTX10002, PTX10008, PTX10016)** Specify the hold-time value to delay the advertisement of up and down transitions (flapping) on an interface.

  [See hold-time.]

- **Increase in the number of supported aggregated Ethernet (ae-) interfaces to 256 from 128**(PTX1000, PTX5000, PTX10002, PTX10008, and PTX10016)

  [See Aggregated Ethernet Interfaces.]

- **Supported transceivers, optical interfaces, and DAC cables** (ACX Series, EX Series, PTX Series, MX Series, and QFX Series).—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

- What's Changed in Release 21.4R2 | **157**
- What's Changed in Release 21.4R1 | **159**

Learn about what changed in this release for PTX Series routers.

What's Changed in Release 21.4R2

IN THIS SECTION

- General Routing | **158**
- Network Management and Monitoring | **158**
- User Interface and Configuration | **158**

VPNs | 159

General Routing

- OpenConfig container names for Point-to-Multipoint per interface ingress and egress sensors are modified for consistency from "signalling" to "signaling".

Network Management and Monitoring

- **Change in behavior of SNMP MIB object ifAlias**—SNMP MIB object ifAlias now shows the configured interface alias. In earlier releases, ifAlias used to show configured interface description.
- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

User Interface and Configuration

- Support for temperature sensor (PTX10001-36MR)—We support the temperature sensor statement at the **edit chassis cb** hierarchy level. You can use the temperature sensor statement to increase the fan speed and customize the temperature threshold. We recommend certain values for ZR and ZR-M modules to work which helps the temperature to remain within the thresholds.

  [See temperature-sensor .]

VPNs

- **Changes to `show mvpn c-multicast` and `show mvpn instance` outputs**—The FwdNh output field displays the multicast tunnel (mt) interface in the case of Protocol Independent Multicast (PIM) tunnels.

  [See `show mvpn c-multicast`.]

What's Changed in Release 21.4R1

IN THIS SECTION

- EVPN | **159**
- General Routing | **159**
- Interface and Chassis | **160**
- Network Management and Monitoring | **160**

EVPN

- **Output for show Ethernet switching flood extensive command** The output for `show ethernet-switching flood extensive` now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as unilist. Previously, the output for `show ethernet-switching flood extensive` would misidentify the next-hop type as composite.

General Routing

- **No support for PKI operational mode commands on the Junos Limited version (MX Series routers, PTX Series routers, and SRX Series devices)**— We do not support `request` , `show` , and `clear` PKI-related operational commands on the limited encryption Junos image ("Junos Limited"). If you try to execute PKI operational commands on a limited encryption Junos image, then an appropriate error message is displayed. The `pkid` process does not run on Junos Limited version image. Hence, the limited version does not support any PKI-related operation.

- On PTX1K and PTX10002-60C the show chassis hardware details command now displays information about USB devices. In addition, information about disk drives is only displayed when the extensive switch is used with the show vmhost hardware operational mode command.

- **Juniper Agile Licensing (EX2300-VC, EX3400-VC, EX4300-VC, EX4400-24MP, EX4400-48MP, PTX10003, PTX10016, QFX5130-32CD, QFX5110-32Q, QFX5110-48S, QFX5120-48T, QFX5210-64C, QFX5200, and QFX5220)**—Starting from this release onwards, the Juniper Agile

License Manager is deprecated. You can use the Juniper Agile Licensing Portal to activate, install, manage, and monitor licenses on Juniper Networks devices.

[See Juniper Agile Licensing Guide.]

- **Renamed veriexec-check option**—We have changed the `veriexec-check` option of the `request system malware-scan` command to `integrity-check`. This update does not include any functional changes. You can use the `integrity-check` option to check whether integrity mechanisms are enabled for the Juniper Malware Removal Tool.

  [See request system malware-scan.]

- **New Commit check for Layer 2 Interfaces (PTX10003)**— We've introduced a commit check to prevent you from misconfiguring ethernet encapsulation on Layer 2 interfaces. Ethernet encapsulation is not supported on Layer 2 interfaces.

  [See encapsulation (Logical Interface)

Interface and Chassis

- When configuring multiple flexible tunnel interface (FTI) tunnels, the source and destination address pair needs to be unique only among the FTI tunnels of the same tunnel encapsulation type. Prior to this PR, the source and destination address pair had to be unique among all the FTI tunnels regardless of the tunnel encapsulation type.

Network Management and Monitoring

- **Limits increased for the `max-datasize` statement (ACX Series, PTX Series, and QFX Series)**—The `max-datasize` statement's minimum configurable value is increased from 23,068,672 bytes (22 MB) to 268,435,456 bytes (256 MB), and the maximum configurable value is increased from 1,073,741,824 (1 GB) to 2,147,483,648 (2 GB) for all script types. Furthermore, if you do not configure the `max-datasize` statement for a given script type, the default maximum memory allocated to the data segment portion of a script is increased to 1024 MB. Higher limits ensure that the device allocates a sufficient amount of memory to run the affected scripts.

  [See max-datasize.]

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.

Known Limitations

IN THIS SECTION

- General Routing | 161

Learn about known limitations in Junos OS Release 21.4R2 for PTX Series routers.

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

General Routing

- The following error message is observed during LC1101 reboot: pechip_cmerror_set_error:3113: Level: Major, cmerror_code: 0x210613 (id=1555). PR1268678
- JFlow cannot handle traffic with multiple Explicit NULL labels. When sampled traffic has two Explicit NULL labels, the packets are dropped and the trapstats increment. PR1601552

Open Issues

IN THIS SECTION

- General Routing | 162
- MPLS | 163
- User Interface and Configuration | 163

Learn about open issues in Junos OS Rlease 21.4R2 for PTX Series routers.

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

General Routing

- On the PTX Platform with FPC-PTX-P1-A or FPC2-PTX-P1A, you might encounter a single event upset (SEU) event that might cause a linked-list corruption of the TQCHIP. The following syslog message gets reported: Jan 9 08:16:47.295 router fpc0 TQCHIP1: Fatal error pqt_min_free_cnt is zero Jan 9 08:16:47.295 router fpc0 CMSNG: Fatal ASIC error, chip TQ Jan 9 08:16:47.295 router fpc0 TQ Chip::FATAL ERROR!! from PQT free count is zero Jan 9 08:16:47.380 router alarmd[2427]: Alarm set: FPC color=RED, class=CHASSIS, reason=FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 Jan 9 08:16:47.380 router craftd[2051]: Fatal alarm set, FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 The Junos OS Chassis Management error handling detects such a condition, raises an alarm, and disables the affected Packet Forwarding Engine entity. To recover this Packet Forwarding Engine entity, restart the FPC. Contact your Juniper support representative if the issue persists even after the FPC restarts. PR1254415

- In the platform using INH (indirect next hop, such as Unilist) as route next hop type for multiple paths scenario (such as BGP PIC or ECMP), the session fast-reroute might be enabled in Packet Forwarding Engines (PFEs). When the version-id of session-id of INH is above 256, the PFE might not respond to session update, which might cause the session-id permanently to be stuck with the weight of 65535 in PFE. It might lead PFE to have a different view of Unilist against load-balance selectors. Then either the BGP PIC or the ECMP-FRR might not work properly and traffic might be dropped or silently discarded. PR1501817

- On PTX Series devices running Junos OS, the JFlow service might not report the accurate throughput rate. This issue is seen when there is high sampled traffic rate with low flow cache hit ratio.PR1502645

- Flapping might be observed on channelized ports of PTX Series routers during ZTP when one of the ports is disabled on the supporting device. PR1534614

- Unsupported configuration is being attempted by the script that then hits the maximum threshold for the given platform. PR1555159

- On PTX platforms, when Inline Jflow is configured and high sampling rate (more than 4000 per second) is set, high CPU utilization might be observed and this might result in relevant impacts on traffic analysis and billing. PR1569229

- On PTX10000 platforms running Junos OS device, file permissions might be changed for /var/db/scripts files after rebooting the device. This issue might have an impact on the scripts running on the box. PR1583839

- In QFX10002-60C device under MAC statistics **output-mac-control-frames** & **output-mac-pause-frames** does not increment. PR1610745

- When a number of routes resolve over an ECMP path, the inline BFD sessions might flap during `clear isis adjacency` command or RPD restart trigger. PR1612802

- V6 default route will not get added after successful dhcpv6 client binding on PTX1000 devices during ZTP. PR1649576
- Fetching SR JVision sensors for for aggregate Ethernet IL per member link stats will not reset after doing the restart routing.PR1652372
- Range field of gre_key flt_type was incorrectly mapped to legacy TOS for DSCP.PR1652762

MPLS

- On PTX3000 devices, if RPD thrashes during a GRES switchover, there might be traffic loss on MPLS LSPs. PR1590681

User Interface and Configuration

- File delete with regular expression might fail, if using filename without regular expression works. PR1624562

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.4R2 | **164**
- Resolved Issues: 21.4R1 | **165**

Learn about the issues fixed in this release for PTX Series routers.

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

Resolved Issues: 21.4R2

IN THIS SECTION

- General Routing | **164**
- Interfaces and Chassis | **165**
- Layer 2 Ethernet Services | **165**
- MPLS | **165**
- Platform and Infrastructure | **165**
- Routing Protocols | **165**

General Routing

- FIPS mode is not supported. PR1530951
- IS-IS adjacency is not coming up through TCC l2circuit. PR1590387
- On PTX devices, inconsistency in the platform name used in multiple places, version, snmp mibs, etc. PR1597999
- Traffic loss might be observed with some MPLS labels in multipath BGP scenarios. PR1618507
- EAPol packets over Layer 2 circuit might get dropped at the tunnel start. PR1628196
- On PTX devices, ddos-protection protocols group ARP counters not showing correct values. PR1629097
- SNMP trap message for FPC restart shows FRU removal instead of Fru Offline/Fru Power off. PR1629738
- Multiple link flaps and traffic might be lost on the links. PR1630006
- RPD core might be observed with warm-standby configurations due to reference counting issues. PR1631871
- SPMB might crash immediately after a switchover. PR1637950
- CCL:NGPR: RPD_KRT_RESPOSE_ERROR: krt change failed for prefix <> error from kernel is "EINVAL -- Bad parameter in request PR1638745
- MAC-VRF does not support MAC limit configuration. PR1647327

Interfaces and Chassis

- After USB upgrade, primary role is getting resolved but FPC's are not coming online.PR1637636

Layer 2 Ethernet Services

- Aggregated Ethernet interface remains up instead of down after deleting loopback and ae interface IP on neighbor while verifying BFD sessions on router. PR1640240

MPLS

- Unexpected traffic loss on LSP headend might be observed when downstream IGP metric changes. PR1625438

Platform and Infrastructure

- On PTX platforms, vmcore on primary Routing Engine might be reported due to mbuf corruption. PR1602442

Routing Protocols

- The rpd might crash and restart when NSR is enabled. PR1620463
- The rpd might crash after clearing IS-IS database. PR1631738
- The BGP route might still be present in the multi-path route after increased IGP cost. PR1643665

Resolved Issues: 21.4R1

IN THIS SECTION

- General Routing | **166**
- Interfaces and Chassis | **168**
- Layer 2 Ethernet Services | **168**
- MPLS | **168**
- Network Management and Monitoring | **169**
- Routing Policy and Firewall Filters | **169**
- Routing Protocols | **169**
- User Interface and Configuration | **169**

General Routing

- Routing Engine switchover does not work as expected while solid-state drive (SSD) failure occurs.PR1437745
- The device might run out of service post GRES or unified ISSU. PR1558958
- MPLS jflow packets are dropped on the MPLS interfaces. PR1559390
- Upgrading PTX1000 platforms with unified SSDs (2x32G SSD) might result in boot loop in certain scenario. PR1571275
- Mirrored packets get corrupted when a filter is applied with the port-mirror and discard action.PR1576914
- File permissions are changed for **/var/db/scripts** files after reboot on PTX platforms. PR1583839
- High FPC CPU utilization might be seen on PTX10002-60C platform. PR1585728
- The **RPD_KRT_KERNEL_BAD_ROUTE** error message is seen in certain scenarios when the rpd process restarts or GRES happens when NSR is enabled. This error has no functional impact. PR1586466
- The na-grpc process crash might be seen and existing telemetry connections will be disconnected. PR1587956
- PTX1000 RCB FIPS 140-2 Level 1 - certification support. PR1590640
- The l2cpd agent might become unresponsive after starting the telemetry service. PR1592473
- Layer 2 VPN stops forwarding when interface encapsulation is changed to `vlan-ccc` from `ethernet-ccc` and back. PR1595455
- [MPC10E] messages log will be filled with **Temp Sensor Fail** alarm set/clear and **cmtfpc_cpu_core_temp_get: Fail to get temp CPU7_PMB** messages. PR1597798
- On PTX10001-36MR platforms, inconsistency in the platform name used in multiple places, version, snmp mibs, etc. PR1597999
- On PTX10008 routers, the EVPN-VXLAN shared tunnel commands must be removed. PR1598142
- On PTX1000 platforms, sFlow data (for example: inner VLAN and outer VLAN value, forwarding-class, and DSCP value) is not exported while checking from server flow records at the collector for ingress sampling. PR1598263
- The unilist nexthop might get stuck after interface flap on PTX. PR1598309
- False fan failure alarm flaps (set and cleared) frequently. PR1599183

- CRC errors increase continuously after interface flap. PR1600768
- Traffic might get silently dropped and discarded due to the RS Fatal error on FPC-PTX-P1-A, FPC2-PTX-P1A, FPC-SFF-PTX-P1-A, and FPC-SFF-PTX-T. PR1600935
- The l2circuit packets with PVST and RPVST destination multicast MAC might get dropped. PR1601360
- OutputInt=0 in JFLOW data reported to collector. PR1601531
- The IPv6 traffic might get impacted on the PTX platforms when an IPv6 route resolves over a dynamic tunnel. PR1602007
- Junos OS, PTX10002-60C System: After upgrading, configured firewall filters might be applied on incorrect interfaces (CVE-2021-31382). PR1602292
- FPC is not fully offline after FPC BAD_VOLTAGE fault is reported. PR1602556
- In Junos OS, an l2cpd memory leak can occur when specific LLDP packets are received leading to a DoS (CVE-2022-22172). PR1602588
- Packet loss might be seen on filter-based GRE deployments. PR1603453
- Traffic loss might be seen on the device due to the continuous errors happening on Fabric Healing process (FHP) phase-1. PR1603499
- The **discard** and redirect function might not take effect if changing action from **then redirect x.x.x.x** to **then discard** or vice-versa. PR1603872
- The FPC `pic-mode` configuration might not be committed successfully. PR1605148
- Link flaps might be observed momentarily on PTX5000 platforms. PR1606008
- Memory leaks might be observed on the l2cpd process when you perform certain LLDP operations. PR1608699
- MACsec session might be dropped due to one way congestion. PR1611091
- The **FPC 0 Major Errors** alarm might be seen on PTX10002-60C due to a rare timing issue. PR1613229
- Line-cards might be unstable due to the continuous growing memory usage of evo-cda-bt app. PR1614952
- VCCV for LDP signaled pseudowire goes down periodically on PTX10008 and PTX10004 with Junos OS. PR1615419
- 90% traffic got dropped when the number of Switch Interface Board (SIB) plane is reduced from 4 to 3 on PTX10008 and PTX10016. PR1615942

- Slow memory leak (32 bytes each time) of rpd might be seen. PR1616065
- Memory leak might be seen when LLDP is configured.PR1617151
- While migration from Junos OS to Junos OS Evolved, customer have to delete chassis redundancy failover or set chassis redundancy failover **disable**. PR1617720
- Performance of Jflow service might be impacted on PTX platforms. PR1617932
- /interfaces/interface/subinterfaces/subinterface/state/counters not exported during initial sync for on-change. PR1620160
- EAPol packets over l2circuit might get dropped at the tunnel start. PR1628196
- RPD core might be observed with warm-standby configurations due to reference counting issues. PR1631871

Interfaces and Chassis

- Junos telemetry interface optics sensor's alarm data type changed from **bool_val to str_val**. PR1580113

Layer 2 Ethernet Services

- Uneven traffic distribution might be observed between member links of LAG. PR1599029
- BFD hold-down timer does not work properly when LAG is configured. PR1616764

MPLS

- Soft-Preemption does not work after applying `subscription 0` configuration on the RSVP interfaces. PR1587177
- The LDP replication session might not get synchronized when the dual-transport is enabled.PR1598174
- VPLS connection might get down if the dual-transport statement is configured.PR1601854
- LDP does not support policy import with rib-groups. PR1611081
- IPv4 Prefixes might be associated into both IPv4 and IPv6 LDP database after Routing Engine switchover. PR1611338
- The RPD crash might happen due to reference count leak in routing table metrics. PR1615001

Network Management and Monitoring

- OC timezone configuration not reflecting in the existing session if Junos timezone configuration in groups is deactivated. PR1608876
- On PTX10008 platforms, syslog does not log information on IPv4 after upgrade. PR1611504

Routing Policy and Firewall Filters

- BGP route preference using PBR is not applied to all the routes when CCNH inet6 is enabled. PR1596436
- Filters in openconfig acl execute terms in the order of their definition and not based on sequence-ids. PR1621620

Routing Protocols

- rpd crash might be seen with Telemetry used setup. PR1607667
- Delay in adding or removing static routes from the router. PR1612173
- Undesired protection path might get selected for some destination prefixes. PR1614683
- The rpd might crash and restart when NSR is enabled. PR1620463

User Interface and Configuration

- The file copy failure is seen via Netconf or operation script. PR1597550
- The commitd core file might be observed after committing some configuration change. PR1601159

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for PTX Series routers.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Basic Procedure for Upgrading to Release 21.4 | 170
- Upgrade and Downgrade Support Policy for Junos OS Releases | 173
- Upgrading a Router with Redundant Routing Engines | 174

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

Starting in Junos OS release 21.2R2, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

Basic Procedure for Upgrading to Release 21.4

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

NOTE: Back up the file system and the currently active Junos OS configuration before upgrading Junos OS. This allows you to recover to a known, stable environment if the upgrade is unsuccessful. Issue the following command:

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

NOTE: The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the router, such as configuration templates and shell scripts (the only exceptions are the juniper.conf and ssh files), might be removed. To preserve the

stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see the Installation and Upgrade Guide.

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

To download and install Junos OS Release 21.4R2:

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

   https://support.juniper.net/support/downloads/

2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the Release drop-down list to the right of the Download Software page.
4. Select the `Software` tab.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new jinstall package on the router.

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

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

```
user@host> request system software add validate reboot source/junos-install-ptx-
x86-64-21.4R1.9.tgz
```

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

```
user@host> request system software add validate reboot source/junos-install-ptx-
x86-64-21.4R1.9-limited.tgz
```

Replace the source with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: You need to install the Junos OS software package and host software package on the routers with the RE-PTX-X8 Routing Engine. For upgrading the host OS on this router with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.

NOTE: After you install a Junos OS Release 21.4 jinstall package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the jinstall package that corresponds to the previously installed software.

NOTE: Most of the existing `request system` commands are not supported on routers with RE-PTX-X8 Routing Engines. See the VM Host Software Administrative Commands in the Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

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

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

Table 6: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Upgrading a Router with Redundant Routing Engines

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

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

For the detailed procedure, see the Installation and Upgrade Guide.

Junos OS Release Notes for QFX Series

IN THIS SECTION

- What's New | 175
- What's Changed | 186
- Known Limitations | 188
- Open Issues | 190
- Resolved Issues | 194
- Documentation Updates | 204
- Migration, Upgrade, and Downgrade Instructions | 205

These release notes accompany Junos OS Release 21.4R2 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

- What's New in 21.4R2 | 175
- What's New in 21.4R1 | 177

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

What's New in 21.4R2

IN THIS SECTION

- EVPN | 175

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

EVPN

- **EVPN-VXLAN fabric with an IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, you can configure an EVPN-VXLAN fabric with an IPv6 underlay. You can use this feature only with MAC-VRF routing instances (all service types). You must configure either an IPv4 or an IPv6 underlay across the EVPN instances in the fabric; you can't mix IPv4 and IPv6 underlays in the same fabric.

To enable this feature, configure the underlay VXLAN tunnel endpoint (VTEP) source interface in the MAC-VRF instance as an IPv6 address. However, you must use the IPv4 loopback address as the router ID for BGP handshaking to work.

This feature was introduced in Junos OS Release 21.2R2.

[See EVPN-VXLAN with an IPv6 Underlay and Understanding EVPN with VXLAN Data Plane Encapsulation.]

- **DHCP relay in an EVPN-VXLAN fabric with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, EVPN-VXLAN fabrics with an IPv6 underlay support DHCP relay. You can configure the DHCP relay agent in centrally routed and edge-routed bridging overlays. Support for DHCP relay includes support for DHCPv4 and DHCPv6. This feature was introduced in Junos OS Release 21.2R2.

  [See DHCP Relay Agent over EVPN-VXLAN.]

- **CoS support for EVPN-VXLAN with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, you can configure CoS features, which enable you to prioritize traffic, on an EVPN-VXLAN fabric with an IPv6 underlay. This feature was introduced in Junos OS Release 21.2R2.

  [See CoS Support on EVPN VXLANs.]

- **Support for firewall filters on EVPN-VXLAN with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos OS Release 21.4R1, QFX5120 switches support firewall filters for ingress and egress traffic on EVPN-VXLAN with an IPv6 underlay. This feature was introduced in Junos OS Release 21.2R2.

  [See Understanding EVPN with VXLAN Data Plane Encapsulation.]

- **Support for EVPN-VXLAN group-based policies (QFX5120-48Y, QFX5120-48YM, QFX5120-48T, and QFX5120-32C)**—Starting in Junos OS Release 21.4R1, QFX5120 switches provide standards-based multilevel segmentation (also called group-based policy, or GBP) on the basis of Layer 3 virtual networks and group-based tags rather than IP-based filters. GBP supports an application-centric policy model that separates network access policies from the underlying network topology through the use of policy tags, thus allowing different levels of access control for endpoints and applications even within the same VLAN.

  The QFX5120 switches also provide GBP support for locally switched traffic on VXLAN access ports.

  [See Example: Micro and Macro Segmentation using Group Based Policy in a VXLAN.]

- **Symmetric integrated routing and bridging (IRB) with EVPN Type 2 routes (QFX5210)**—Starting in Junos OS Release 21.4R1, you can enable symmetric IRB EVPN Type 2 routing on QFX5210 switches in an EVPN-VXLAN ERB overlay fabric. With the symmetric routing model, leaf devices can route and bridge traffic on both ingress and egress sides of a VXLAN tunnel. To do this, the leaf

devices use a special transit VXLAN network identifier (VNI) and Layer 3 interfaces on the associated VLAN to exchange traffic across the VXLAN tunnels.

We support this feature with:

- EVPN instances configured using MAC-VRF routing instances.
- VLAN-aware bundle or VLAN-based Ethernet service types.
- EVPN Type 5 routing using Layer 3 virtual routing and forwarding (VRF) instances with IRB interfaces for intersubnet reachability.

This feature was introduced in Junos OS Release 21.3R1-S1.

[See Symmetric Integrated Routing and Bridging with EVPN Type 2 Routes in EVPN-VXLAN Fabrics and Using a RIOT Loopback Port to Route Traffic in an EVPN-VXLAN Network.]

What's New in 21.4R1

IN THIS SECTION

- EVPN | **178**
- High Availability | **179**
- Juniper Extension Toolkit (JET) | **180**
- Junos Telemetry Interface (JTI) | **180**
- Licensing | **180**
- MPLS | **181**
- Network Management and Monitoring | **181**
- Operation, Administration, and Maintenance (OAM) | **182**
- Routing Policy and Firewall Filters | **182**
- Routing Protocols | **183**
- Services Applications | **184**
- Additional Features | **185**

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

EVPN

- **EVPN-VXLAN fabric with an IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, you can configure an EVPN-VXLAN fabric with an IPv6 underlay. You can use this feature only with MAC-VRF routing instances (all service types). You must configure either an IPv4 or an IPv6 underlay across the EVPN instances in the fabric; you can't mix IPv4 and IPv6 underlays in the same fabric.

  To enable this feature, configure the underlay VXLAN tunnel endpoint (VTEP) source interface in the MAC-VRF instance as an IPv6 address. However, you must use the IPv4 loopback address as the router ID for BGP handshaking to work.

  This feature was introduced in Junos OS Release 21.2R2.

  [See EVPN-VXLAN with an IPv6 Underlay and Understanding EVPN with VXLAN Data Plane Encapsulation.]

- **DHCP relay in an EVPN-VXLAN fabric with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, EVPN-VXLAN fabrics with an IPv6 underlay support DHCP relay. You can configure the DHCP relay agent in centrally routed and edge-routed bridging overlays. Support for DHCP relay includes support for DHCPv4 and DHCPv6. This feature was introduced in Junos OS Release 21.2R2.

  [See DHCP Relay Agent over EVPN-VXLAN.]

- **CoS support for EVPN-VXLAN with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, you can configure CoS features, which enable you to prioritize traffic, on an EVPN-VXLAN fabric with an IPv6 underlay. This feature was introduced in Junos OS Release 21.2R2.

  [See CoS Support on EVPN VXLANs.]

- **Support for firewall filters on EVPN-VXLAN with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos OS Release 21.4R1, QFX5120 switches support firewall filters for ingress and egress traffic on EVPN-VXLAN with an IPv6 underlay. This feature was introduced in Junos OS Release 21.2R2.

  [See Understanding EVPN with VXLAN Data Plane Encapsulation.]

- **Support for EVPN-VXLAN group-based policies (QFX5120-48Y, QFX5120-48YM, QFX5120-48T, and QFX5120-32C)**—Starting in Junos OS Release 21.4R1, QFX5120 switches provide standards-based multilevel segmentation (also called group-based policy, or GBP) on the basis of Layer 3 virtual networks and group-based tags rather than IP-based filters. GBP supports an application-centric policy model that separates network access policies from the underlying network topology through the use of policy tags, thus allowing different levels of access control for endpoints and applications even within the same VLAN.

The QFX5120 switches also provide GBP support for locally switched traffic on VXLAN access ports.

[See Example: Micro and Macro Segmentation using Group Based Policy in a VXLAN.]

- **Symmetric integrated routing and bridging (IRB) with EVPN Type 2 routes (QFX5210)**—Starting in Junos OS Release 21.4R1, you can enable symmetric IRB EVPN Type 2 routing on QFX5210 switches in an EVPN-VXLAN ERB overlay fabric. With the symmetric routing model, leaf devices can route and bridge traffic on both ingress and egress sides of a VXLAN tunnel. To do this, the leaf devices use a special transit VXLAN network identifier (VNI) and Layer 3 interfaces on the associated VLAN to exchange traffic across the VXLAN tunnels.

  We support this feature with:

  - EVPN instances configured using MAC-VRF routing instances.
  - VLAN-aware bundle or VLAN-based Ethernet service types.
  - EVPN Type 5 routing using Layer 3 virtual routing and forwarding (VRF) instances with IRB interfaces for intersubnet reachability.

  This feature was introduced in Junos OS Release 21.3R1-S1.

  [See Symmetric Integrated Routing and Bridging with EVPN Type 2 Routes in EVPN-VXLAN Fabrics and Using a RIOT Loopback Port to Route Traffic in an EVPN-VXLAN Network.]

High Availability

- **Unified ISSU support on QFX5120-48Y**—Starting in Junos OS Release 21.4R1, QFX5120-48Y switches support unified in-service software upgrade (ISSU). The unified ISSU feature enables you to upgrade between two different Junos OS releases with minimal disruption on the control plane and with minimal disruption of traffic.

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

  > **NOTE**: QFX5120-48Y switches provide unified ISSU support only if the Cancun versions of the chipset SDK are the same for the current version and the version you are upgrading to. See, No Link Title.

  [See Getting Started with Unified In-Service Software Upgrade and Understanding In-Service Software Upgrade (ISSU).]

Juniper Extension Toolkit (JET)

- **Support for programming FTIs using JET APIs (PTX1000, PTX10002, PTX10008, PTX10016, QFX5100, and QFX10008)**—Starting in Junos OS Release 21.4R1, you can use the Interfaces Service API to configure flexible tunnel interfaces (FTIs) in Junos OS. You can change the attributes of the tunnel configurations for the unit under an existing FTI but cannot change the existing tunnel encapsulation type using the APIs. For the following families, you can configure only the listed attributes when you use JET APIs:

  - `inet` and `inet6`: `address` and `destination-udp-port`
  - `mpls` and `iso`: `destination-udp-port`

  [See Overview of JET APIs and Configure Flexible Tunnel Interfaces.]

Junos Telemetry Interface (JTI)

- **Packet Forwarding Engine performance sensors (EX4650, QFX5110, QFX5120-48Y, QFX5200, and QFX5210)**—Starting in Junos OS Release 21.4R1, JTI streams NPU utilization statistics by means of remote procedure calls (gRPC), gRPC network management interface (gNMI), or UDP (native) transport from a device to an outside collector.

  [See sensor (Junos Telemetry Interface), Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface), and Telemetry Sensor Explorer.]

Licensing

- **License renewal or automatic update (EX2300, EX3400, EX4300, EX4400-24MP, PTX10001-36MR, PTX10003, PTX10008, PTX10016, QFX5130-32CD, QFX5220, vMX, and vSRX)**—Starting in Junos OS Release 21.4R1, you can renew or automatically update all software feature licenses using the following commands:

  - `set system license autoupdate url <link>`
  - `set system license renew before-expiration <days>`
  - `set system license renew interval <hours>`

  The `license autoupdate` and `license renew` commands streamline license tracking. Use these commands to reduce the manual tracking effort for license renewal.

  [See License Autoupdate and License Renew.]

MPLS

- **Support for optimizing auto-bandwidth adjustments for MPLS LSPs (QFX10008)**—Starting in Junos OS Release 21.4R1, you can configure faster auto-bandwidth adjustment for MPLS LSPs under overflow or underflow conditions. This feature decreases the minimum allowed value of `adjust-threshold-overflow-limit` and `adjust-interval` to 150 seconds when `adjust-threshold-overflow-limit` and `adjust-threshold-underflow-limit` cross the configured threshold values. In releases before Junos OS Release 21.4R1, the `adjust-interval` value is 300 seconds under overflow or underflow conditions.

  You can configure a faster in-place LSP bandwidth update that avoids signaling of a new LSP instance as part of make-before-break. To configure, include the `in-place-lsp-bandwidth-update` configuration statement at the `[edit protocols mpls label-switched-path` *`lsp-name`*`]` hierarchy level.

  You can also configure RSVP interfaces to support subscription percentage per priority. To configure, include the `subscription priority` *`priority`* `percent value` configuration statement at the `[edit protocols rsvp interface` *`interface-name`*`]` hierarchy level.

  [See Configuring Optimized Auto-bandwidth Adjustments for MPLS LSPs.]

Network Management and Monitoring

- **Remote port mirroring to IPv6 address (EX4650, EX4650-48Y-VC, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—Starting in Junos OS Evolved Release 21.4R1, you can use remote port mirroring to copy packets entering or exiting a port or entering a VLAN and send the copies to the IPv6 address of a device running an analyzer application on a remote network (sometimes referred to as *extended port mirroring*). When you use remote port mirroring to an IPv6 address, the mirrored packets are GRE-encapsulated.

  Add the address you would like to have the copied packets sent to in the CLI hierarchy. For example, `set forwarding-options analyzer ff output ip-address 2000::1`.

  [See Understanding Port Mirroring and Analyzers.]

- **Support for port mirroring and analyzers with Layer 3 VXLAN gateway (QFX5210)**—Starting in Junos OS Release 21.4R1, the QFX5210 supports port mirroring when used as a Layer 3 VXLAN gateway. However, the QFX5210 does not support true egress mirroring. Packet contents are different when you configure egress mirroring on the network port. Layer 2 fields in the mirrored packets are undefined, and you should not consider those fields for validation.

  [See Port Mirroring and Analyzers and Using a RIOT Loopback Port to Route Traffic in an EVPN-VXLAN Network.]

Operation, Administration, and Maintenance (OAM)

- **Enhancements to Bidirectional Forwarding Detection (BFD)-triggered fast reroute (FRR) for unicast next hops and session-id-change-limiter-indirect (MX Series, PTX1000, PTX3000, PTX5000, PTX10001, PTX10002, PTX10016, QFX10002-60C, QFX10002, QFX10008, QFX10016, and vMX)** —In Junos OS Release 21.4R1, we've enhanced the BFD-triggered fast reroute (FRR) for unicast next hops and session-id-change-limiter-indirect to address the issue of traffic being silently discarded because of a session mismatch between the control plane and data plane.

  To limit the re-programming of the number of parent nodes of the indirect-nexthop and avoid additional the complexity in the Packet Forwarding Engine when the session-identifier id of the indirect nexthop is changed, use the `session-id-change-limiter-indirect` configuration statement at the `[edit routing-options]` hierarchy level.

  [See Bidirectional Forwarding Detection (BFD) for MPLS.]

Routing Policy and Firewall Filters

- **Support for IPv4 and IPv6 firewall filters on Layer 3 gateways in EVPN-VXLAN fabrics (QFX5210)**— Starting in Junos OS Release 21.4R1, QFX5210 switches acting as Layer 3 gateways in EVPN-VXLAN fabrics support IPv4 and IPv6 firewall filters in the ingress direction of the IRB interface. We recommend that you do not apply filters on the RIOT loopback interface. The switch supports the following match conditions:

  - `source-address`
  - `destination-address`
  - `source-port`
  - `destination-port`
  - `ttl`
  - `ip-protocol`
  - `hop-limit`

  The supported actions are:

  - `accept`
  - `discard`
  - `log`
  - `syslog`

- `policer`

  The QFX5210 does not support filter-based forwarding (FBF).

  [See Firewall Filter Match Conditions and Actions (QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX5700, EX4600, EX4650).]

- **Support for source-port and destination-port range optimize conditions to reduce the TCAM space**—Starting in Junos OS Release 21.4R1, we support the `source-port-range-optimize` and the `destination-port-range-optimize` conditions at the `[edit firewall family ethernet-switching filter <filter-name> term <term-name> from]` hierarchy level. This configuration considerably reduces the ternary content addressable memory (TCAM) space usage. QFX Series line of switches support up to 24 non-contiguous matching conditions for the `source-port-range-optimize` and `destination-port-range-optimize` options.

  [See Firewall Filter Match Conditions and Actions (QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX5700, EX4600, EX4650).]

Routing Protocols

- **Higher DDoS bandwidth for Layer 2 and Layer 3 protocols (PTX1000, PTX10002, PTX10008, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, we support higher distributed denial-of-service (DDoS) bandwidth for many Layer 2 and Layer 3 protocols.

  [See protocols (DDoS) (ACX Series, PTX Series, and QFX Series).]

- **Remote LFA support for LDP in IS-IS (QFX10000 line of switches)** —Starting in Junos OS Release 21.4R1, you can configure a remote loop-free alternate (LFA) path to extend the backup provided by the LFA route in an IS-IS or OSPF network. This feature is especially useful for Layer 1 metro rings where the remote LFA is not directly connected to the point of local repair (PLR). You can reuse the existing LDP implementation for the MPLS tunnel setup for the protection of IS-IS and OSPF networks and subsequent LDP destinations. By doing this, you eliminate the need for RSVP-TE backup tunnels for backup coverage.

  [See Understanding Remote LFA over LDP Tunnels in IS-IS Networks and Remote LFA over LDP Tunnels in OSPF Networks Overview.

- **OSPF link delay measurement and advertising (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.4R1, you can measure and advertise various performance metrics in IP networks with scalability through probe messages that are sent by Two-Way Active Measurement Protocol (TWAMP) Light. OSPF receives probe messages and the measured values from TWAMP Light. OSPF advertises these messages as TLVs in packets. You can use these metrics to make path-selection decisions based on the network performance.

  [See How to Enable Link Delay Measurement and Advertising in OSPF.]

- **Support for multiple update threads to service a peer group (MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.4R1, you can configure multiple update threads to service a peer group to improve the performance of BGP. You can use the `group-split-size` configuration statement at the `[edit system processes routing bgp update-threading]` hierarchy level and configure a threshold value (0 through 2000).

  [See update-threading.]

- **Support for ICMP extension (QFX5100)**—Starting in Junos OS Release 21.4R1, we've implemented RFC 5837, *Extending ICMP for Interface and Next-Hop Identification*, for both numbered and unnumbered aggregated Ethernet interfaces. We can now append additional fields to the following ICMP (IPv4 and IPv6) messages:

  - ICMPv4 Time Exceeded
  - ICMPv4 Destination Unreachable
  - ICMPv6 Time Exceeded
  - ICMPv6 Destination Unreachable

  Use the `set system allow-icmp4-extension` command to enable ICMP extension.

  [See Configure ICMP Features.]

Services Applications

- **Inband Flow Analyzer (IFA) 2.0 (QFX5120-48Y and QFX5120-32C)**—In Junos OS Release 21.4R1, we've introduced support for IFA 2.0 on QFX Series switches. IFA 2.0 monitors and analyzes packets entering and exiting the network. You can use IFA 2.0 to monitor the network for faults and performance issues. IFA 2.0 supports both Layer 3 and VXLAN flows.

  With IFA 2.0, you can collect various flow-specific information from the data plane, without the involvement of the control plane or the host CPU. IFA collects data on a per-hop basis across the network. You can export this data to external collectors to perform localized or end-to-end analytics.

  IFA 2.0 contains three different processing nodes:

  - IFA initiator node
  - IFA transit node
  - IFA terminating node

  [See Inband Flow Analyzer (IFA) 2.0 Probe for Real-Time Performance Monitoring, inband-flow-telemetry, show services inband-flow-telemetry, and clear inband-flow-telemetry stats.]

Additional Features

We've extended support for the following features to these platforms.

- **EVPN-VXLAN support** (QFX5120-48YM):
  - EVPN-VXLAN with MAC-VRF routing instances
  - Filter-based forwarding in EVPN-VXLAN
  - IPv6 data traffic support through an EVPN-VXLAN overlay network
  - IPv6 support for firewall filtering and policing on EVPN-VXLAN traffic
  - Port mirroring and analyzers on EVPN-VXLAN
  - Storm control on EVPN-VXLAN

  [See EVPN User Guide.]

- **EVPN Type 2 and Type 5 route coexistence** (EX9200, EX9251, EX9253, MX204, MX240, MX480, MX960, MX2010, MX10003, MX10008, and QFX10002-60C)

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

- **MACsec bounded delay protection** (EX4400 and SRX380)

  [See bounded-delay.]

- **MACsec timer-based SAK refresh** (QFX5120-48YM)

  [See sak-rekey-interval.]

- **Storm control in an EVPN-VXLAN fabric with Layer 3 gateway** (QFX5210)

  > **NOTE:** We recommend that you do not configure storm control on the aggregated Ethernet interface used as the loopback port to support RIOT functionality.

  [See Understanding Storm Control.]

- **Support for Precision Time Protocol (PTP) G.8275.2 enhanced profile with PTP over IPv4 and IPv6 unicast traffic** (QFX5120-48T)

  [See G.8275.2 Enhanced Profile.]

- **Support for sFLow with EVPN-VXLAN Layer 3 gateway** (QFX5210)

[See sFlow Monitoring Technology and Using a Default Layer 3 Gateway to Route Traffic in an EVPN-VXLAN Overlay Network.]

- **Supported transceivers, optical interfaces, and DAC cables** (ACX Series, EX Series, PTX Series, MX Series, and QFX Series).—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

- What's Changed in Release 21.4R2 | 186
- What's Changed in Release 21.4R1 | 187

Learn about what changed in this release for QFX Series Switches.

What's Changed in Release 21.4R2

IN THIS SECTION

- Network Management and Monitoring | 186
- VPNs | 187

Network Management and Monitoring

- **Change in behavior of SNMP MIB object ifAlias**—SNMP MIB object ifAlias now shows the configured interface alias. In earlier releases, ifAlias used to show configured interface description.
- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

- When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
- When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

[See Enable and Configure Instances of the Ephemeral Configuration Database.]

VPNs

- **Changes to `show mvpn c-multicast` and `show mvpn instance` outputs**—The FwdNh output field displays the multicast tunnel (mt) interface in the case of Protocol Independent Multicast (PIM) tunnels.

  [See `show mvpn c-multicast`.]

What's Changed in Release 21.4R1

IN THIS SECTION

- EVPN | 187
- Network Management and Monitoring | 188

EVPN

- **Community information no longer included in VRF routing table**—The QFX series switches will no longer include the inherited advertised route target communities, EVPN extended communities, or vxlan encapsulation communities for EVPN Type 2 and EVPN Type 5 routes when an IP host is added in the VRF routing table.
- **Output for the show Ethernet switching flood extensive command**—The output for the `show ethernet-switching flood extensive` command now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as unilist. Previously, the output for the `show ethernet-switching flood extensive` command would misidentify the next-hop type as composite.

Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.

- **Limits increased for the `max-datasize` statement (ACX Series, PTX Series, and QFX Series)**—The `max-datasize` statement's minimum configurable value is increased from 23,068,672 bytes (22 MB) to 268,435,456 bytes (256 MB), and the maximum configurable value is increased from 1,073,741,824 (1 GB) to 2,147,483,648 (2 GB) for all script types. Furthermore, if you do not configure the `max-datasize` statement for a given script type, the default maximum memory allocated to the data segment portion of a script is increased to 1024 MB. Higher limits ensure that the device allocates a sufficient amount of memory to run the affected scripts.

  [See max-datasize.]

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.

Known Limitations

IN THIS SECTION

- General Routing | **189**
- Infrastructure | **189**

Learn about known limitations in Junos OS Release 21.4R2 for QFX Series switches.

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

General Routing

- On QFX1000 devices, source MAC and TTL values are not updated for routed multicast packets in EVPN-VXLAN. PR1346894
- On the QFX5000 devices with storm control, there is a significant difference between the configured rate and the actual rate. PR1526906
- On QFX5200 and QFX5100 devices with the IP-IP tunnel feature, `show dynamic-tunnels database statistics` command output shows extra packet counts (i.e. sampled packets when sFlow is enabled). PR1555922
- On QFX5000 devices, in EVPN-VXLAN deployment, Broadcast, Unknown Unicast, and Multicast (BUM) traffic replication over VTEP might send out more packets than expected. PR1570689
- On QFX5000 devices, IRACL filters are unable to match the VxLAN tunnel terminated packets. PR1594319
- The 1pps performance test fails on the copper ports.PR1618533
- When the IFA2.0 init feature enabled on the device and flows are sampled, incorrect pps and bps statistics gets displayed at the logical child interface level on the ingress and egress ports. PR1620139
- Junos OS does not support the unified ISSU on QFX5120-48Y devices if there is a change in the Cancun versions of the chipset SDKs between the releases. A change in the Cancun firmware leads to the chip reset impacting unified ISSU. The Cancun versions in the chipset SDKs must be the same between two Junos OS releases for unified ISSU to work.PR1634695

Infrastructure

- Software image upgrade from Junos OS Release 21.1 (or earlier) to Junos OS Release 21.2 (or later) requires no-validate command as a mandatory action. PR1586481

Open Issues

IN THIS SECTION

- EVPN | **190**
- General Routing | **190**
- Infrastructure | **192**
- Interfaces and Chassis | **193**
- Layer 2 Ethernet Services | **193**
- Layer 2 Features | **193**
- Platform and Infrastructure | **193**
- Routing Protocols | **193**
- User Interface and Configuration | **194**

Learn about open issues in Junos OS Release 21.4R2 for QFX Series switches.

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

EVPN

- Need to modify I-ESI workflow on DC-GW.PR1600600
- EVPN local ESI MAC limit might not be effective in some scenarios. PR1619299

General Routing

- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. PR1362609
- PIM-based VXLAN does not work on QFX5110 switches. As a result, traffic loss is seen from VXLAN tunnel to Layer 2 interface. PR1462548

- When running the command `show pfe filter hw filter-name <filter name>`, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. PR1495712
- On devices running Junos OS Release 21.4R2, the JFlow service might not report the accurate throughput rate. This issue is seen when there is high sampled traffic rate with low flow cache hit ratio.PR1502645
- On the QFX5100 devices that does not run the QFX-5E codes (non TVP architecture), when you install the image with vendor SDK upgrade (6.5.X), the CPU utilization might go up by around 5 percent.PR1534234
- On the QFX5000 devices, route leaking does not work for IPv4 routes if the mask is less than 16 and for IPV6 routes if the mask is less than 64.PR1538853
- FPC might not be recognized after power cycle (hard reboot). PR1540107
- On the QFX10002-60c devices, NP-100G-DAC-3M/5M does not start on QFX10002-60C devices.PR1555955
- To avoid the additional interface flap, interface hold time needs to be configured. PR1562857
- In mixed QFX5100, EX4300 VCF setup, duplicate traffic might be observed for some Layer 3 multicast traffic streams. PR1568152
- The OSPF session over IRB might not come up in the EVPN-VXLAN scenario. PR1577183
- On the QFX5100 device Virtual Chassis, the **DHCP ACK** messages do not get generated while verifying Smart Relay with interfaces in the routing instance. PR1581025
- In a fully loaded devices, at times, firewall programming was failing due to scaled prefix configuration with more than 64800 entries. However, this issue is not observed in development setup. PR1581767
- On Junos QFX10000 devices, file permissions might be changed for /var/db/scripts files after rebooting the device. This issue might have an impact on the scripts running on the box. PR1583839
- On the QFX5000 devices, the dcpfe process might crash. PR1588704
- On QFX series, switches with the vendor chip as Packet Forwarding Engine, if IS-IS is enabled on an integrated routing and bridging (IRB) interface and the maximum transmission unit (MTU) size of the IRB interface is configured with a value great than 1496 bytes, the IS-IS hello (IIH) PDUs with jumbo frame size (i.e., great than 1496 bytes) might be dropped and not sent to the IS-IS neighbors. The following is the product list of QFX series switches with vendor chip as Packet Forwarding Engine. QFX3500/QFX3600/QFX5100/QFX5110/QFX5120/QFX5130/QFX5200/QFX5210/QFX5220 PR1595823
- Pim VXLAN does not work on the TD3 chipsets that enables the VXLAN flexflow.PR1597276

- The convergence time degradation is seen in IS-ISv6, OSPFv2, and OSPFv3 when comparing convergence time with Junos OS Release 21.1R1.5. As it is a convergence time issue, many components are involved and hence need investigation of rpd, kernel, and Packet Forwarding Engine. PR1602334
- On QFX5100 devices, optical power is seen after detached and attached QSFP on disable interface. PR1606003
- On the QFX10002-72q devices, the sFlow samples do not get generated for the transit MPLS traffic carrying IPv6..PR1607497
- On the QFX10002-60C devices, the `output-mac-control-frames` and `output-mac-pause-frames` counters do not increase. PR1610745
- On the QFX5100 Virtual Chassis, traffic loss occurs while testing the 118 aggregate Ethernet groups. PR1611162
- On the QFX10002, QFX10008, and QFX10016 devices, on scaling more than 80,000 ARP/NDP, the **prds_jpf_nh_token_change: Token change failed for rnh** error messages gets generated. PR1616224
- When the IFA2.0 init feature enabled on switch and flows are sampled, incorrect pps and bps statistics displayed at the logical child interface level on the ingress and egress ports. PR1620139
- The led port init was done for SXE port. PR1621630
- Secondary FPC lose their connection to the primary when new members are added to the Virtual Chassis Fabric (VCF). PR1634533
- On all QFX Series devices, when any firewall filter is configured with action as **sample** and **accept**, and applied on the Integrated Routing and Bridging (IRB) interface. Then the firewall filter might drop all the inbound traffic.PR1646740
- On Junos devices QFX5100, QFX5110, and QFX5200, when the device is rebooted or the dcpfe process gets restarted with the `local-bias` configuration statement enabled on the aggregate Ethernet interface, then the `local-bias` on the aggregate Ethernet interface does not work as expected. This impacts traffic utilization on the device as the Virtual Chassis (VC) ports might still carry traffic even when the `local-bias` is configured.PR1651151

Infrastructure

- On QFX Series platforms, IPv6 traffic output byte (ipv6-transit-statistics) might not be in expected range as per traffic generator statistics. PR1653671

Interfaces and Chassis

- On the QFX5120 devices, multiple mclag-cfgchkd process generates core files after loading the recent operating system. PR1599025

Layer 2 Ethernet Services

- The DHCP client configuration is coming from two places, that is, AIU script and VSDK sandbox. The DHCP client configuration coming from AIU script has the serial ID in vendor ID where as the default configuration from sandbox doesn't have it. There is no impact on functionality or service. PR1601504

Layer 2 Features

- Adding one more sub-interface logical interface to an existing interface causes 20 to 50 milliseconds traffic drop on the existing logical interface. PR1367488

Platform and Infrastructure

- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect ASIC programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. PR1530160

Routing Protocols

- Multicast traffic is overusing the switch core when igmp-snooping is removed. The MCSNOOPD will generate core files due to the changes in mrouter interfaces and routes. PR1569436
- When the statement `accept-remote-source` under PIM is removed, the PIM SG entries might not be updated with the correct RPF. Clearing of the states would take care of the issue. This is day-1 behavior. PR1593283

- The mcsnoopd process might generate core files at **rt_mcnh_nh_add_del**, **rt_mcnh_nh_add_with_table_id**, **mc_build_nh_for_bd_evpn_extended**, **mc_bd_create_or_update_all_fld_grp_routes**. PR1605393

User Interface and Configuration

- File delete with regular expression might fail, if using filename without regular expression it works. PR1624562

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.4R2 | **194**
- Resolved Issues: 21.4R1 | **199**

Learn about the issues fixed in this release for QFX Series switches.

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

Resolved Issues: 21.4R2

IN THIS SECTION

- Class of Service (CoS) | **195**
- EVPN | **195**
- General Routing | **195**
- Interfaces and Chassis | **198**
- MPLS | **198**
- Platform and Infrastructure | **199**
- Routing Policy and Firewall Filters | **199**

Routing Protocols | 199

Class of Service (CoS)

- The uplink interface remains down for a longer duration due to VXLAN scaled configuration. PR1631448

EVPN

- Few ARP/ND/MAC entries for VLANs are missing with MAC-VRF configuration. PR1609322
- IRB proxy-arp unrestricted might not work if EVPN/l2alm proxy is enabled. PR1613201
- Multiple memory leaks might be seen leading to rpd process crash. PR1626416
- The MAC address might not be visible in the EVPN/VXLAN environment. PR1645591

General Routing

- FIPS mode is not supported. PR1530951
- When soft loopback port and analyzer configurations are committed together, mirror ingress to local port is not working . PR1581542
- During FRR, when more than one multi home interface is down, traffic might loop for QFX5110. PR1596589
- Error message "error: syntax error: request-package-validate" will be seen on device CLI output during non-stop software upgrade. PR1596955
- The dcpfe/FPC process might crash on the QFX10000 Series platforms in a rare case. PR1597479
- The interface on SFP-T or SFP-SX might stop forwarding traffic on EX4600. PR1598805
- EVPN-VXLAN:QFX10008: RE1 went to DB prompt when tried loading profile configurations over LRM configurations. PR1598814
- QFX5200: Observed dcpfe core file while testing unified ISSU from Junos OS Release 21.1R1.11 to Junos OS Release 21.2R1.7. PR1600807
- Removing and adding Virtual Chassis ports might cause the FPC to reboot. PR1601557

- InterDC traffic loss might be seen in MAC-VRF EVI with trap statistics "dlu.ucode.discard". PR1601961
- Chassisd generates "Cannot read hw.chassis.startup_time value: m" every 5 seconds on QFX10008 and QFX10016. PR1603588
- FPC might crash post firewall filter configuration changes in QFX Series platforms. PR1608610
- The ports might remain in downstate on QFX5000 platforms. PR1611354
- ARP resolution for data traffic received over type5 might fail. PR1612905
- FPC might crash after the device restarts in EVPN-VXLAN scenario. PR1613702
- Removing the optical module "JNP-SFPP-10GE-T" from a port might cause certain ports to go down. PR1614139
- The BFD session might flap on the QFX5120-48YM platform. PR1616692
- One-time interface flap might be seen on the QFX5120 platform. PR1618891
- BGP session might not establish between loopback interfaces when routes are learnt through type5 EVPN routes. PR1620642
- EVPN-VXLAN type5 traffic might fail on the Spine device of QFX1000. PR1620924
- Host generated IPv4 traffic sent over IPv6 next-hop with IRB interface might get dropped. PR1623262
- Interface on QFX5200 does not come up after swapping from 100G to 40G. PR1623283
- MACsec session might flap if multiple logical interfaces are created on the single physical interface. PR1624524
- PKID might crash and generate a core file when there is limited memory available on the Routing Engine. PR1624613
- QFX5000 log messages: fpc0 SRIRAM Tx VxLAN Ucast: ifd_out = vtep dst_gport is (c00000X) are observed. PR1624925
- Traffic loss might be observed after configuring VXLAN over IRB interface. PR1625285
- The `no-incoming-port` statement is not applied after reboot on QFX10002 and QFX10008 platforms. PR1625988
- The third 802.1Q tag might not be pushed onto the stack in the Q-in-Q tunneling. PR1626011
- Routing Engine generated traffic might not be forwarded when next-hop is indirect unilist of EVPN type 5 tunnel. PR1627363

- QFX10002-60C platform might not respond back to ICMP packets received with TTL or hop limit value of 1. PR1627566
- Layer 3 traffic failure might be observed with scaled MC-LAG configuration on QFX10002, QFX10008, and QFX10016 platforms. PR1627846
- Traffic loss might be observed due to Address Resolution Protocol (ARP) getting programmed as indirect next-hop by control plane for external routes distributed over IRB on QFX10000 Junos platforms. PR1627876
- 802.1p BA classification might not work on mixed Virtual Chassis when the interface has a DSCP and 802.1p classifier. PR1628447
- DHCP inform ACK might be sent with broadcast address when DHCP smart relay is used. PR1628837
- The vmhost crash might be seen in a rare condition when a route is added or changed. PR1629200
- Some ports (port 20 and above) might not come up on QFX5110-32Q VC after the device restarts or Packet Forwarding Engine reboots. PR1629231
- The interface on the peer device might remain up even after disabling the 10G interface on the Juniper device. PR1629637
- Traffic might get dropped when `family ethernet-switching` is configured on the interface in Q-in-Q scenario. PR1629680
- `show interface extensive` might not show local or remote fault. PR1629735
- LACP timeout might be observed during high CPU utilization. PR1630201
- QFX5000 : Chassis Status LED does not work as described in the document. PR1630380
- Inner VLAN might be stripped off when input-native-vlan-push is disabled. PR1631771
- The interface might remain in the "UP/UP" state even the interface is disabled for administrator. PR1632440
- You might see a slow response or timeout on the CLI or SNMP with accessing to sxe-0/0/0 on QFX5120-48T-6c. PR1632620
- The FBF filtered VLAN traffic will not be passed properly to the forwarding routing instances over aggregated Ethernet interfaces on QFX5000 platforms. PR1633452
- Traffic loss after MAC ages. PR1633879
- The VCPs connected with the AOC cable might not come up after upgrading to Junos OS Release 17.3 or later. PR1633998

- Data might not be exchanged via EVPN-VxLAN domain. PR1635347
- chassisd might crash if chassis disk-partition is configured. PR1635812
- Traffic might silently be dropped or discarded when STP is configured in VxLAN environment. PR1636950
- Configuring L2PT on a transit switch in a Q-in-Q environment breaks L2PT for other S-VLANs. PR1637249
- Delay might be observed for the interfaces to come up after reboot or transceiver replacement. PR1638045
- Targeted broadcast or WOL feature might not work on QFX5000 platforms. PR1638619
- In a VCF scenario on QFX5100, VCP interfaces might flap or not come up at all and CRC errors might increase. PR1639543
- MAC-move might be observed when `dhcp-security` is configured. PR1639926
- MAC address of the hosts might get learned on incorrect VLAN which might lead to traffic loss. PR1639938
- On QFX Series base license is missing after upgrading to Junos OS Release 20.3 and later. PR1640123
- ICMP TTL exceeded packets are not sent out of the switch. PR1643457
- Packets are dropped in ingress QFX5000 with EVPN-LAG multihoming due to VP-LAG programming issue. PR1644152
- VxLAN tunnel termination due to change in configuration. PR1646489
- The VCP link might take longer time to come up during system reboot/Packet Forwarding Engine restarts. PR1651316

Interfaces and Chassis

- `show vrrp extensive` does not show the next logical interface "Interface VRRP PDU statistics". PR1637735
- Traffic loss might be seen for the MAC addresses learned on the ICL interface. PR1639713

MPLS

- MPLS VPN packets drop due to missing ARP entry on PE device. PR1607169

- Unexpected traffic loss on LSP headend might be observed when downstream IGP metric changes. PR1625438
- Traffic towards MPLS core file is not rerouted to alternate port on QFX5000 platforms. PR1627002

Platform and Infrastructure

- The packet drop might be seen on FPC on MX Series based platforms. PR1631313

Routing Policy and Firewall Filters

- The rpd process might get stuck at 100 percent when EVPN vrf-target is enabled and after any configuration change. PR1616167

Routing Protocols

- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific BGP export policies. PR1626367
- The BFD session might go down when multiple addresses of same subnet are configured. PR1635700

Resolved Issues: 21.4R1

IN THIS SECTION

- Class of Service (CoS) | **199**
- EVPN | **200**
- General Routing | **200**
- Infrastructure | **204**
- MPLS | **204**
- Layer 2 Ethernet Services | **204**
- Routing Protocols | **204**

Class of Service (CoS)

- The TCP-ECN traffic might not be forwarded with high priority. PR1585854

EVPN

- Traffic loss might occur under the EVPN scenario when MAC-IP moves from one CE interface to another. PR1591264
- The device announces router-MAC, target, and EVPN VXLAN community to the BGP IPv4 NLRI. PR1600653
- Traffic sent by the QFX5000 leaf to remote leaf with link goes into the `Down` state. PR1605375
- The MAC-table aging timeout fails in some scenarios. PR1612866

General Routing

- Routing Engine switchover does not work as expected when SSD fails. PR1437745
- Unexpected next-hop might occur after the route gets deleted. PR1477603
- The interface might go into the `Blocking` state impacting the traffic when the link-protection switches from primary to backup. PR1555294
- On the QFX5100 line of switches, the Virtual Chassis Port (VCP) might not come up after upgrading to Junos OS Release18.4R2-S4 or later. PR1555741
- On the QFX5110 line of switches, the untagged traffic routed over native-vlan might be dropped. PR1560038
- The na-grpcd process might generate core files during the longevity tests. PR1565255
- The MAC address points to an incorrect interface after traffic stops and not ages out. PR1565624
- On the QFX10000 line of switches, the dcpfe and fpc process might crash if the ARP MAC moves. PR1572876
- On the QFX10K2-60C line of switches, the `disk missing` alarm does not get generated. PR1573139
- On QFX Series switches, when a VRF instance configuration exists and you upgrade to Junos OS Release 20.3 or later and commit the upgrade might generate the `warning: requires 'l3vpn' license"` warning message. PR1575608
- On the QFX10000 line of switches, the port might not be brought down immediately during some abnormal type of line card reboot. PR1577315
- On QFX5000 line of switches, the `show route detail` command might not display the Next-hop type IPoIP Chained comp nexthop in the output. PR1584322
- ARP resolution for data traffic received over Type5 might fail. PR1612905

- The l2cpd process generates a core file with the FIP snooping configuration on any interface. PR1617632
- Junos OS does not support the Dot1x based firewall policers. PR1619405
- On the QFX5100 line of switches, some 40G ports might not be channelized successfully. PR1582105
- On the QFX5000 line of switches, the firewall filter does not get programmed after you delete a large filter and add a new one in a single commit. PR1583440
- File permissions changes for the **/var/db/scripts** files after a reboot. PR1583839
- On the QFX10002-60C line of switches, high FPC CPU utilization might occur. PR1585728
- On the QFX5210-64C line of switches, the PSU firmware upgrades through Junos OS. PR1589572
- On the QFX5120 line of switches, the MPLS traffic might not be forwarded after the aggregate interface flaps. PR1589840
- The Virtual Chassis mastership changes and the connection drops after renumbering the backup member ID. PR1590358
- On the QFX5120-48T line of switches after removing 1G speed on interfaces, the interface does not come back as 10G. PR1591038
- Routing Engine kernel might crash due to logical interface of the aggregated interface, adding failure in the Junos OS kernel. PR1592456
- The IPv4 fragmented packets might be broken if you configure PTP transparent clock. PR1592463
- The BFD session might flap during the Routing Engine switchover. PR1593244
- The dcpfe process might crash in the EVPN-VXLAN scenario. PR1593950
- Packet might drop in the ECMP next-hop flap scenario. PR1594030
- ARP entry might be missed intermittently after FPC reboots. PR1594255
- The label field for the EVPN Type-1 route gets set to 1. PR1594981
- The re-installation of the Type-5 tunnels might fail in the EVPN-VXLAN scenario. PR1595197
- The DCI InterVNI and IntraVNI traffic might be silently discarded in the gateway node due to the tagged underlay interfaces. PR1596462
- The mcscnoopd process might crash when you delete or add the Layer 2 forwarding configuration after ISSU. PR1596483

- The `fpc0 bcm pkt reinsert failed` log gets generates in the log messages in an aggressive way. PR1596643
- Traffic might be dropped after the backup FPC reboots in a Virtual Chassis scenario. PR1596773
- The interface might not be brought up when you configure QinQ. PR1597261
- Deletion of MACsec configuration on an logical interface does not work. PR1597848
- The socket connection drops as the keepalive timer expires with port 33015. PR1598019
- On the QFX5000 line of switches, sFlow impacts on ICMP traffic. PR1598239
- On the OFX5100, QFX5110, QFX5120, QFX5200, and QFX5210 line of switches, the DDoS violations might be reported for the IP multicast miss traffic (IPMCAST-MISS) incorrectly. PR1598678
- File permissions changes for the **/var/db/scripts** files after reboot. PR1599365
- On the QFX10002-60C line of switches, the Layer 3 traffic silently gets discarded with the IRB interface. PR1599692
- Not able to disable the management port em1. PR1600905
- On QFX5120-48y-8c line of switches, the dcpfe process generates core file while issuing the `show pfe vxlan nh-usage` command in the ERB EMC scenario with around 6000 ARP entries. PR1601949
- InterDC traffic loss might occur in the MAC-VRF EVI with the `dlu.ucode.discard` trap status. PR1601961
- The IPv6 traffic might be impacted when an IPv6 route resolves over a dynamic tunnel. PR1602007
- Under certain scaling scenarios with EVPN-VXLAN configurations, the l2ald process might be aborted and then recovered. PR1602244
- The egress interface of the GRE tunnel does not dynamically get updated when the destination to tunnel changes. PR1602391
- FPC goes into the `Down` state and the dcpfe process might generate core file in some cases. PR1602583
- Traffic loss might occur in the MC-LAG scenario. PR1602811
- On the QFX5000 line of switches, traffic might be dropped in the Virtual Chassis scenario when you configure the firewall filter. PR1602914
- On the QFX5120 line of switches, traffic gets mirrored even after deactivating the analyzer configuration. PR1603192

- Unicast DHCP packets might get flooded when you configure the DHCP relay in the non-default routing-instance. PR1603444
- Packet loss might occur on the filter-based GRE deployments. PR1603453
- Duplicate packets might appear when you bring up all the interfaces on the spine switch. PR1604393
- The carrier transition counter might not get incremented upon link flap after the reboot. PR1605037
- MAC might move between the ICL and MC-LAG interface if you add or remove VLANs on the ICL interface. PR1605234
- Multicast streams might stop flooding in the VXLAN setup. PR1606256
- The Virtual Chassis ports might remain in the `Down` state after you remove and add the ports. PR1606705
- The LLDP packets received on VXLAN-enabled port might be flooded unexpectedly. PR1607249
- The fxpc process might crash and generate a core file. PR1607372
- Ping to lo0/IRB over Type-5 fails. PR1610093
- On the QFX10000 line of switches, continuous Layer 3 traffic might drop with the MC-LAG configuration. PR1610173
- The QFX Virtual Chassis might lose license on Junos OS Release 21.2R1. PR1610272
- On the QFX10002-60C line of switches, continuous FPC might crash and the dcpfe process might generate core file. PR1612871
- On the QFX5000 line of switches, the VLAN firewall filter does not get deleted in the Packet Forwarding Engine after configuration changes. PR1614767
- The l2ald process might crash in the EVPN scenario. PR1615269
- The BFD session might get become nonresponsive in the `Init` state after l2-learning restart due to incomplete ARP resolutions. PR1618280
- Disabled VCP (Virtual chassis port) might go into the `Up` state after the optic is reseated. PR1619997
- Traffic might be lost after configuring VXLAN over the IRB interface. PR1625285
- Need to implement the `show task scheduler-slip-history` command to display the number of the scheduler slips and the last 64 slip details. PR1626148

Infrastructure

- The `Host 0 Active Disk Usage Exceeded` alarm might be generated due to large files, which were already marked as deleted. PR1601251

MPLS

- On the QFX5000 line of switches, traffic loss occurs after the STP topology changes. PR1616878

Layer 2 Ethernet Services

- Traffic received on a port in the LACP `Detached` state might be incorrectly forwarded. PR1582459
- The DHCP client might become offline for about 120 seconds after sending the `DHCPINFORM` message. PR1587982

Routing Protocols

- The remaining BFD sessions of the aggregated Ethernet interface flaps continuously if one of the BFD sessions gets deleted. PR1516556
- The IPv4 static route might still forward traffic unexpectedly even when the static route configuration has already been deleted. PR1599084
- On the QFX10002 line of switches, the verification of BGP peer count fails after deleting the BGP neighbors. PR1618103
- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific BGP export policies. PR1626367

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for QFX Series switches.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 217

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

Starting in Junos OS release 21.2R2, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

Upgrading Software on QFX Series Switches

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

If you are not familiar with the download and installation process, follow these steps:

1. In a browser, go to https://www.juniper.net/support/downloads/junos.html.

   The Junos Platforms Download Software page appears.

2. In the QFX Series section of the Junos Platforms Download Software page, select the QFX Series platform for which you want to download the software.

3. Select **20.3** in the Release pull-down list to the right of the Software tab on the Download Software page.

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 20.3 release.

   An Alert box appears.

5. In the Alert box, click the link to the PSN document for details about the software, and click the link to download it.

A login screen appears.

6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Download the software to a local host.
8. Copy the software to the device or to your internal software distribution site.
9. Install the new jinstall package on the device.

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

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

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-20.3-R1.n-secure-signed.tgz reboot
```

Replace *source* with one of the following values:

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

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

Rebooting occurs only if the upgrade is successful.

> **NOTE**: After you install a Junos OS Release 20.3 `jinstall` package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

This section explains how to upgrade the software, which includes both the host OS and the Junos OS. This upgrade requires that you use a VM host package—for example, a **junos-vmhost-install-*x*.tgz** .

During a software upgrade, the alternate partition of the SSD is upgraded, which will become primary partition after a reboot .If there is a boot failure on the primary SSD, the switch can boot using the snapshot available on the alternate SSD.

NOTE: The QFX10002-60C switch supports only the 64-bit version of Junos OS.

NOTE: If you have important files in directories other than /config and /var, copy the files to a secure location before upgrading. The files under /config and /var (except /var/etc) are preserved after the upgrade.

To upgrade the software, you can use the following methods:

If the installation package resides locally on the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-20.4R1.9.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-
x86-64-20.4R1.9.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-x86-64-20.4R1.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-x86-64-20.4R1.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-
x86-64-20.4R1.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-
x86-64-20.4R1.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)

outing Engine status:
  Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
```

Performing a Unified ISSU

You can use unified ISSU to upgrade the software running on the switch with minimal traffic disruption during the upgrade.

NOTE: Unified ISSU is supported in Junos OS Release 13.2X51-D15 and later.

Perform the following tasks:

- No Link Title
- No Link Title

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

- Ensure that nonstop active routing (NSR), nonstop bridging (NSB), and graceful Routing Engine switchover (GRES) are enabled. NSB and GRES enable NSB-supported Layer 2 protocols to synchronize protocol information between the master and backup Routing Engines.

  To verify that nonstop active routing is enabled:

  > **NOTE**: If nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

  ```
  user@switch> show task replication
          Stateful Replication: Enabled
          RE mode: Master
  ```

  If nonstop active routing is not enabled (`Stateful Replication` is `Disabled`), see Configuring Nonstop Active Routing on Switches for information about how to enable it.

- Enable nonstop bridging (NSB). See Configuring Nonstop Bridging on EX Series Switches for information on how to enable it.

- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the `request system snapshot` command.

Upgrading the Software Using Unified ISSU

This procedure describes how to upgrade the software running on a standalone switch.

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in Installing Software Packages on QFX Series Devices.
2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:

- On the switch, enter:

```
user@switch> request system software in-service-upgrade /var/tmp/package-name.tgz
```

where *package-name*.tgz is, for example, jinstall-host-qfx-10-f-x86-64-20.4R1.n-secure-signed.tgz.

NOTE: During the upgrade, you cannot access the Junos OS CLI.

The switch displays status messages similar to the following messages as the upgrade executes:

```
warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get lost!
ISSU: Validating Image
ISSU: Preparing Backup RE
Prepare for ISSU
ISSU: Backup RE Prepare Done
Extracting jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz ...
Install jinstall-host-qfx-5-f-x86-64-19.2R1.n-secure-signed.tgz completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status                  Reason
  FPC 0          Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
```

```
ISSU: IDLE
Initiate em0 device handoff
```

NOTE: A unified ISSU might stop, instead of abort, if the FPC is at the warm boot stage. Also, any links that go down and up will not be detected during a warm boot of the Packet Forwarding Engine (PFE).

NOTE: If the unified ISSU process stops, you can look at the log files to diagnose the problem. The log files are located at `/var/log/vjunos-log.tgz`.

5. Log in after the reboot of the switch completes. To verify that the software has been upgraded, enter the following command:

```
user@switch> show version
```

6. Ensure that the resilient dual-root partitions feature operates correctly, by copying the new Junos OS image into the alternate root partitions of all of the switches:

```
user@switch> request system snapshot slice alternate
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

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

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

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

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

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

Table 7: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for SRX Series

IN THIS SECTION

- What's New | 219
- What's Changed | 225
- Known Limitations | 230
- Open Issues | 231
- Resolved Issues | 233
- Documentation Updates | 244
- Migration, Upgrade, and Downgrade Instructions | 244

These release notes accompany Junos OS Release 21.4R2 for the SRX Series Services Gateways. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

- What's New in 21.4R2 | **219**
- What's New in 21.4R1 | **219**

Learn about new features introduced in this release for SRX Series Gateways.

What's New in 21.4R2

There are no new features or enhancements to existing features in Junos OS Release 21.4R2 for SRX Series Gateways.

What's New in 21.4R1

IN THIS SECTION

- Application Identification (AppID) | **220**
- Authentication and Access Control | **220**
- Chassis | **220**
- Chassis Cluster-specific | **221**
- Flow-Based and Packet-Based Processing | **221**
- Hardware | **221**
- J-Web | **222**
- Network Address Translation (NAT) | **223**
- Platform and Infrastructure | **223**

Software Installation and Upgrade | 224
Unified Threat Management (UTM) | 224
Additional Features | 225

Learn about new features introduced in this release for SRX Series Gateways.

Application Identification (AppID)

- **Dual stacking of IPv4 and IPv6 (SRX Series and vSRX)**—Starting in Junos OS Release 21.4R1, we support dual stacking of IPv4 and IPv6 addresses for overlay and underlay networks in an AppQoE configuration.

  [See Support for IPv6 Traffic in AppQoE.]

Authentication and Access Control

- **LDAP authentication for Juniper Secure Connect (SRX Series devices and vSRX with Juniper Secure Connect)**—In Junos OS Release 21.4R1, we've introduced support for native LDAP authentication with secure connection to simplify deployments of Juniper Secure Connect. With the LDAP authentication support, you can determine which groups should be granted access after successful authentication. Use the `address-assignment` option at the `[edit access profile profile-name authentication-order ldap ldap-options]` hierarchy level to assign IP addresses specifically for those groups of users to simplify IP address management.

  [See ldap-options.]

Chassis

- **Support for FPC major alarm (SRX5400, SRX5600, and SRX5800 with SPC3)**—In Junos OS Release 21.4R1, we've enhanced the following commands to show more details about the FPC major alarm:

  - `show chassis error active`
  - `show chassis error active detail`
  - `show chassis error active fpc-slot` *`slot-number`*
  - `show chassis error active detail fpc-slot` *`slot-number`*

  You can use these commands to identify and troubleshoot the hardware issues.

[See show chassis errors active.]

- **Increase in AC redundancy mode to 2+2 for high-capacity high-line PEMs (SRX5400)**—Starting in Junos OS Release 21.4R1, the SRX5400 device supports 2+2 AC redundancy mode on high-capacity high-line power entry modules (PEMs). The support for 2+2 redundancy mode increases the PEM's capacity from 2050 W to 4100 W.

  [See SRX5400 Services Gateway AC Power Supply Specifications.]

Chassis Cluster-specific

- **Support for external 10GbE ports on SCB2, SCB3, SCB4 (SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.4R1, you can connect the HA control links in a chassis cluster using external 10GbE ports on SCB2, SCB3, or SCB4. The Ethernet ports are supported on these types of Switch Control Boards (SCB) as HA control ports. The control link traffic can bypass the SPCs to increase the resiliency of the chassis cluster.

  [See Understanding SCB Control Links and Chassis Cluster Dual Control Links.]

Flow-Based and Packet-Based Processing

- **Express Path+ for Layer 2 secure-wire traffic (SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.4R1, we've added support for Express Path+ to secure-wire interfaces. This support allows the SRX device to automatically accelerate the flow traversing secure-wire interfaces with their network processor, increasing throughput and decreasing latency.

  [See Express Path.]

- **Support for fat flow (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 21.4R1, we support fat flow technology to improve the firewall and NAT throughput value up to 10 times of the current value.

  [See Understanding Symmetric Fat IPsec Tunnel.]

Hardware

- **High-capacity second-generation AC PSM for SRX5800**—Starting in Junos OS Release 21.4R1, SRX5800 supports the new high-capacity second-generation AC power supply module (PSM). This single or dual feed PSM provides a maximum output power of 5100 W. In single-feed mode, the PSM provides power at a reduced capacity (2550 W). In dual feed mode, the PSM provides power at full capacity (5100W). The PSM supports 1+1 redundancy.

  High-voltage second-generation Universal PSM for SRX5800—Starting in Junos OS 21.4R1, the SRX5800 supports the new high-voltage second-generation universal power supply module (PSM).

This single feed PSM provides a maximum output power of 5100W, and supports either AC or DC input. The PSM supports 1+1 redundancy.

The increased power supply capacity enables SRX5800 devices to support service cards like SPC3. `show chassis power` command displays PSM status, including state, input type, feed, capacity, output, and remaining power. `show chassis environment pem` command displays the power entry module (PEM) status for state, temperature, AC/DC input, and AC/DC output for the SRX5800 device.

[See show chassis power and show chassis environment.]

J-Web

- **Support for Adaptive Threat Profiling in security and IPS policies (SRX Series)**—Starting in Junos OS Release 21.4R1, we support Adaptive Threat Profiling for security and intrusion prevention system (IPS) policy rules.

  When creating security policy rules:

  - Under Source and Destination, you can configure source and destination identity feeds.
  - Under Advanced Settings, you can configure source and destination IP addresses to the feed.

  When creating IPS policy rules, you can configure attacker and target IP addresses to the feed.

  [See Add a Rule and Add Rules to an IPS Policy.]

- **Enhanced IPS Policies page (SRX Series)**—In Junos OS Release 21.4R1, we've refreshed the IPS Policies page for better experience. You can:

  - Drag and drop a selected policy to change the order.
  - Search for policies using the Search icon.
  - Add IPS signatures using the new simplified Predefined or Custom tabs.
  - Navigate directly to the Security Policies page to associate the selected IPS policies.
  - When creating IPS policy rules, you can add attacker and target IP addresses.

  [See About the IPS Policies Page.]

- **New Security Package Management page (SRX Series)**—Starting in Junos OS Release 21.4R1, you can configure and manage IPS signatures, application signatures, and URL categories at our one-stop shop, the Security Package Management page. You can access this page at **Device Administration** > **Security Package Management**.

  We've removed the following options and pages to avoid duplication:

  - Dynamic Applications page:

    - Removed the **Download** button and the **Uninstall/Install** link.
    - Removed the **Download** section from the Global Settings page.
  - Security Services menus:
    - Removed the Web Filtering Category Update page from Security Services > UTM.
    - Removed the Signature Update page from Security Services > IPS.

  [See About the Security Package Management Page.]

- **Enhanced filtering support on the Monitor Logs pages (SRX Series)**—Starting in Junos OS Release 21.4R1, you can choose many filter values to filter the logs and events on the following pages under Monitor > Logs:
  - Session
  - Threats
  - Web Filtering
  - ATP
  - All Events

  [See Monitor Session and Monitor Threats.]

Network Address Translation (NAT)

- **Enhancements to source NAT pool IP address range and NAT pool name character length (SRX Series and MX-SPC3)**—Starting in Junos OS Release 21.4R1, we've increased the source NAT pool IP address range from 8 IP addresses to 64 IP addresses.

  We've also increased the configurable length of the source NAT pool name, destination NAT pool name, source NAT rule name, destination NAT rule name, static NAT rule name, and rule set name from 31 characters to 63 characters.

  [See show security nat source rule, show security nat destination rule, and show security nat static rule.]

Platform and Infrastructure

- **PKI usability enhancements (MX240, MX480, MX960, SRX Series, and vSRX)**—Starting in Junos OS Release 21.4R1, we've enhanced PKI commands to provide additional details about the local and certificate authority (CA)-issued certificates. With these enhancements, you can:

- View the CA certificate status of a CA profile group using the `request security pki ca-profile-group-status ca-group-name group-name` command. See request security pki ca-profile-group-status.
- Configure certificate automatic reenrollment trigger time in days, hours, or percentage using the `set security pki auto-re-enrollment cmpv2 certificate-id certificate-id-name re-enroll-time (days value| hours value| percentage value)` or `set security pki auto-re-enrollment scep certificate-id certificate-id-name re-enroll-time (days value| hours value| percentage value)` command. See auto-re-enrollment.
- View the CA chain, SHA256 fingerprint, and certificate serial number (hexadecimal and decimal format) for a local certificate using the `show security pki local certificate <cert_id> detail` command. See show security pki local-certificate (View).
- View the CA profile associated with a CA certificate and SHA256 fingerprint using the `show security pki ca-certificate <brief|detail>` command. See show security pki ca-certificate (View).
- View additional verification information about local and CA certificate using the `request security pki local-certificate verify` and the `request security pki ca-certificate verify` command, respectively. See request security pki ca-certificate verify (Security) and request security pki local-certificate verify (Security).
- View more PKI-related statistics using the `show security pki statistics` command. Clear the PKI statistics using the `clear security pki statistics` command. See show security pki statistics and clear security pki statistics.

Software Installation and Upgrade

Unified Threat Management (UTM)

- **Content filtering based on file content (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 21.4R1, content security (UTM) performs content filtering to determine the file type based on the file content and not on file extensions. The file content is first analyzed to accurately determine the file type.

  This feature replaces the legacy content filtering based on MIME type, content type, and protocol commands.

  You can define the content filtering rule-set and rules from the `[edit security utm utm-policy <utm-policy-name> content-filtering]` hierarchy and use these rules from the `[edit security utm default-configuration content-filtering]` hierarchy for controlling the traffic direction.

  The existing `show security utm content-filtering statistics` command is enhanced to display the content filtering system statistics and errors.

  [See Content Filtering, content-filtering (Security UTM Policy), utm, and utm default-configurationshow security utm content-filtering statistics.]

Additional Features

We've extended support for the following features to these platforms.

- **Configure concurrent connections** (SRX Series devices and vSRX running iked). Configure the number of concurrent connections that the group profile supports using the `connections-limit` configuration statement at the `[edit security ike gateway gateway-name dynamic]` hierarchy level. We support this configuration for both IKEv1 and IKEv2. This configuration is applicable only to AutoVPN, ADVPN, dynamic endpoint, and remote access (preshared-key and PKI-based tunnels).

  There are no restrictions on the number of connections accepted if you haven't configured the `connections-limit` option.

  [See dynamic (Security)].

- **Dynamic routing protocols** (MX240, MX480, and MX960 with MX-SPC3, SRX5000 line of devices with SPC3 card and vSRX running iked). We support the exchange of dynamic routing information through IPsec VPN tunnels. You can now enable the dynamic routing protocol, such as OSPF, BGP, BFD, PIM, and RIP on a st0 interface of an IPsec VPN tunnel.

  This feature is supported only if the `junos-ike` package is installed in your device.

  [See Routing Protocols Support on IPsec VPN Tunnels.]

- **MACsec bounded delay protection** (EX4400 and SRX380)

  [See bounded-delay.]

What's Changed

IN THIS SECTION

- What's Changed in Release 21.4R2 | **226**
- What's Changed in Release 21.4R1 | **227**

Learn about what changed in this release for SRX Series Gateways.

What's Changed in Release 21.4R2

IN THIS SECTION

- Authentication and Access Control | 226
- J-Web | 226
- Network Management and Monitoring | 226
- Unified Threat Management (UTM) | 227

Authentication and Access Control

- **Enhanced UAC authentication (SRX Series)**—To regulate the lifespan (default 60 seconds) of event table entries, we've added a new configuration statement set services unified-access-control event-table-lifetime time interval in seconds> . If there is a delay in authentication at the SRX Series device, use this configuration statement to enable UAC traffic after the user is authorized from the IC.

  [See Configuring Junos OS Enforcer Failover Options (CLI Procedure).]

J-Web

- **Changes in Identity Management page (SRX Series)**—Starting in Junos OS Release 21.4R1, we've renamed Identity Management as Juniper Identity Management Services (JIMS) in the following location: In Security Services > Firewall Authentication, the Identity Management menu is renamed to JIMS. In Identity Management page (new JIMS page), all instances of Identity Management are renamed to Juniper Identity Management Services.

Network Management and Monitoring

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

- When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

[See Enable and Configure Instances of the Ephemeral Configuration Database.]

Unified Threat Management (UTM)

- **Content filtering CLI updates (SRX Series and vSRX)**—We've the following updates to the content filtering CLI:
  - Trimmed the list of file types supported for content filtering rule match criteria. Instead of uniquely representing different variants of a file type, now only one `file-type` string represents all variants. Hence, the `show security utm content-filtering statistics` output is also updated to align with the new file types available in the rule match criteria.
  - Renamed the content filtering security logging option `seclog` to `log` to match with the Junos OS configuration standard.
  - Rephrased the `reason` string associated with content filtering security log message.

  [See content-filtering (Security UTM Policy), content-filtering (Security Feature Profile), and show security utm content-filtering statistics.]

What's Changed in Release 21.4R1

IN THIS SECTION

- General Routing | **228**
- J-Web | **228**
- Network Management and Monitoring | **228**
- Platform and Infrastructure | **228**
- Routing Protocols | **229**
- Unified Threat Management (UTM) | **229**
- VPNs | **229**

General Routing

- **No support for PKI operational mode commands on the Junos Limited version (MX Series routers, PTX Series routers, and SRX Series devices)**— We do not support `request` , `show` , and `clear` PKI-related operational commands on the limited encryption Junos image ("Junos Limited"). If you try to execute PKI operational commands on a limited encryption Junos image, then an appropriate error message is displayed. The `pkid` process does not run on Junos Limited version image. Hence, the limited version does not support any PKI-related operation.

J-Web

- **Changes to the Dashboard and Monitor pages (SRX Series)**—To improve the J-Web UI loading speed:
  - On the Dashboard page, we've removed the on-box reports related widgets.
  - On the Monitor > Maps and Charts > Traffic Map page, we've changed the default duration from "Last 1 hour" to Last "5 minutes".
- **Changes in Identity Management page (SRX Series)**—Starting in Junos OS Release 21.4R1, we've renamed Identity Management as Juniper Identity Management Services (JIMS) in the following location:
  - In Security Services > Firewall Authentication, the Identity Management menu is renamed to JIMS.
  - In Identity Management page, all instances of Identity Management are renamed to Juniper Identity Management Services.

Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.

Platform and Infrastructure

- Advanced anti malware hash feature is deprecated.
- **Enhanced UAC authentication (SRX Series)**—To regulate the lifespan (default 60 seconds) of event table entries, we've added a new configuration statement set services unified-access-control event-table-lifetime time interval in seconds> . If there is a delay in authentication at the SRX Series device, use this configuration statement to enable UAC traffic after the user is authorized from the IC.

[See Configuring Junos OS Enforcer Failover Options (CLI Procedure).]

Routing Protocols

- The RPD_OSPF_LDP_SYNC message not logged?On all Junos OS and Junos OS Evolved devices, when an LDP session goes down there is a loss of synchronization between LDP and OSPF. After the loss of synchronization, when an interface has been in the holddown state for more than three minutes, the system log message with a warning level is sent. This message appears in both the messages file and the trace file. However, the system log message does not get logged if you explicitly configure the `hold-time` for `ldp-synchronization` at the **`edit protocols ospf area area id interface interface name`** hierarchy level less than three minutes. The message is printed after three minutes.

- To achieve consistency among resource paths, the resource path /mpls/signalling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter**ip-addr='address'**/state/counters**name='name'**/out-pkts/ is changed to /mpls/signaling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter**ip-addr='address'**/state/counters**name='name'**/. The leaf "out-pkts" is removed from the end of the path, and "signalling" is changed to "signaling" (with one "l").

Unified Threat Management (UTM)

- **Default action hit output field for UTM Web filtering statistics (SRX Series)**—We've introduced a new `Default action hit` output field for the `show security utm web-filtering statistics` operational command. The `Default action hit` output field displays the number of sessions for which the juniper-local, juniper-enhanced, or websense-redirect profiles took the default action.

  [See show security utm web-filtering statistics.]

VPNs

- **Deprecated Dynamic VPN CLI configuration statements and operational commands (SRX Series Devices)**—Starting in Junos OS Release 21.4R1, we’ve deprecated the dynamic VPN remote access solution. This means that you cannot use Pulse Secure Client on these devices.

  As part of this change, we’ve deprecated the `[edit security dynamic-vpn]` hierarchy level and its configuration options. We’ve also be deprecated the `show` and `clear` commands under the `[dynamic-vpn]` hierarchy level.

  As an alternative, you can use the Juniper Secure Connect remote access VPN client that we introduced in Junos OS Release 20.3R1. Juniper Secure Connect is a user-friendly VPN client that supports more features and platforms than dynamic VPN does. SRX comes with two built-in concurrent users on all SRX Series devices. If you need additional concurrent users, then contact

your Juniper Networks representative for remote-access licensing. To understand more about Juniper Secure Connect licenses, see Licenses for Juniper Secure Connect and Managing Licenses.

[See Juniper Secure Connect User Guide, Juniper Secure Connect Administrator Guide, Licenses for Juniper Secure Connect, and Managing Licenses.]

Known Limitations

Learn about known limitations in Junos OS Release 21.4R2 for SRX Series Gateways.

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

Flow-Based and Packet-Based Processing

- Use an antireplay window size of 512 for IPv4 or IPv6 in fat-tunnel. The ESP sequence check might otherwise report out-of-order packets if the fat-tunnel parallel encryption is within 384 packets (12 cores * 32 packets in one batch). Hence, there are no out-of-order packets with 512 antireplay window size. PR1470637

J-Web

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

Platform and Infrastructure

- SRX Series devices might encounter ISSU aborted with error "ISSU is not supported for Clock Synchronization (SyncE)" during upgrades from any release prior to Junos OS release 22.1 to 22.1 or above releases. PR1632810

VPNs

- In some scenario (for example, configuring firewall filter), routers might show obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. PR1432925
- An IPsec policy must not have both ESP and AH proposals. The configuration will commit, but the IPsec traffic will not work. Do not configure an IPsec policy with proposals using both ESP and AH protocols. PR1552701

Open Issues

Learn about open issues in Junos OS Release 21.4R2 for SRX Series Gateways.

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

Chassis Clustering

- HA AP mode on-box logging in logical systems and tenant systems, the intermittently security log contents of binary log file in logical systems and tenant systems are not as expected. PR1587360
- When creating a HA cluster setup, secondary node interfaces are not displayed. PR1636002

Flow-Based and Packet-Based Processing

- For accelerated flows such as Express Path, the packet or byte counters in the session close log and show session output take into account only the values that accumulated while traversing the NP. PR1546430

Interfaces and Chassis

- Traffic drop might be seen on irb interface on SRX1500 devices for network control forwarding class when verifying dscp classification based on single and multiple code-points. PR1611623

Network Address Translation (NAT)

- In AA mode with NAT configuration, on RG failover, traffic getting dropped on SRX Series devices. PR1636596

Platform and Infrastructure

- In macOS platforms, when the client connects successfully, the client is not getting minimized to the tray icon and it stays connected and you need to manually minimize it. PR1525889
- HTTP sessions takes approximately 10 minutes to re-establish after a link flap between hub and spoke. PR1577021
- With SSL proxy configured along with Web proxy, the client session might not closed on the device even though proxy session ends gracefully. PR1580526

- On SRX Series devices, if the SNMP packet (traps or polls) has to cross multiple routing-instances, it will cause the packet to be dropped due to incorrect routing-instance ID added by SRX Series devices.PR1616775
- The pkid process pause due to null pointer dereferencing during local certificate verification in some cases. PR1624844
- For LTE interfaces (dl0, cl-*) on security devices, configured in a High Availability cluster mode if redundancy failover is performed then user might lose connection to the internet. If redundancy failover is not performed then no issue is seen. PR1625125
- On the SRX4100 and SRX4200 platforms, it can detect DPDK Tx stuck issue and trigger a major chassis alarm goes which might trigger RG1 failover to the healthy node. A DPDK reset will be triggered only to the stuck port and if the reset resolves the tx stuck issue.PR1626562
- LACPD generates core files sometimes when member links are swapped between two reth bundle using rollback operation given that prior to rollback each of the bundle already has maximum number of child links. PR1632371
- SMTPS sessions are not getting identified when traffic is sent from IXIA (BPS) profile. PR1635929
- The remote-access-juniper-std license might not get freed up while disconnect or reconnect after RG0 failover. PR1642653
- The AAMW action log are not observed when setting log-notifications sometimes. PR1644000
- Authentication entries will not be synchronized to secondary node in the HA setup and when switchover happens, already established authentication sessions will be lost and clients will have to login again with authentication credentials. PR1651129
- The firewall authentication with user firewall based RADIUS access has system logs missing the username and rule. PR1654842

VLAN Infrastructure

- For SOF Layer 2 secure wire session, if the macOS move happen on an existing offloaded session, the packet sent out by SRX Series devices will carry old macOS address and causing traffic drop on end user. PR1597681

VPNs

- On SRX5400, SRX5600, and SRX5800 devices, during in-service software upgrade (ISSU), the IPsec tunnels flap, causing a disruption of traffic. The IPsec tunnels recover automatically after the ISSU process is completed. PR1416334

- In some scenarios, the SRX5000 line of devices might show obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. PR1432925
- Tunnel debugging configuration is not synchronized to the backup node. It needs to be configured again after RG0 failover. PR1450393
- IPsec rekey fails when the SRX Series device is configured with kilobyte-based lifetime in remote access solution. PR1527384
- First time when we add this command the existing active connections are not changed, only the new connection after this command will be taken into effect. PR1608715
- Fragment packets through policy based IPsec tunnel could be dropped in some rare case when PMI is enabled. PR1624877

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.4R2 | **233**
- Resolved Issues: 21.4R1 | **238**

Learn about the issues fixed in this release for SRX Series Gateways.

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

Resolved Issues: 21.4R2

Authentication and Access Control

- The authentication delay might occur upto 60 seconds if same user authenticates. PR1626667

Chassis Clustering

- Secondary node in a chassis cluster might go into reboot loop on SRX Series devices. PR1606724
- SPU might become offline on standby node after failover in SRX Series device chassis cluster. PR1624262

- The Create Bearer Request might be dropped on SRX Series devices. PR1629672
- BFD over high availability ICL link might flap. PR1631938
- Post a series of actions MNHA functionality might not be available despite the configuration presence. PR1638794

Flow-Based and Packet-Based Processing

- The services offload packets processed counter not incremented in security flow statistics. PR1616875
- The flowd process might generate core files if route change or delete in PMI mode. PR1624707
- Packets may not be classified according to the CoS rewrite configuration. PR1634146
- The process nsd may stop continuously due to failure in creating or reinitializing the file /var/db/ext/monitor-flow-cfg. PR1638008
- On SRX 4600 and SRX5000 line of devices running Junos OS release 21.3R1 or later, when Express Path and Power Mode Express Path (PME) are enabled at the same time, the sessions may not be properly offloaded to the Trio ASIC's and device performance may suffer as a result. PR1652025

General Routing

- PKID core might occur during cert signature validation. This core is not very frequent and occurs due to memory corruption. PR1573892
- The fxp0 interface of an SRX550 device in cluster might become unreachable from an external network. PR1575231
- BGP adjacency might not get established in Layer 2 with IRB scenario. PR1582871
- Getting UNKNOWN instead of HTTP-PROXY for application and UNKNOWN instead of GOOGLE-GEN in RT-FLOW close messages These messages can be seen in the RT-flow close log and these are due to JDPI not engaged for the session. This may affect the app identification for the web-proxy session traffic. PR1588139
- On Juniper Secure Client, the traffic gets dropped during reaching Juniper Secure Connect installed client from server behind gateway in TCP path finder enabled VPN gateway. PR1611003
- Execute RSI on SRX5000 line of devices with IOC2 card installed may trigger data plane failover. PR1617103
- On SRX Series devices using On-Box Logging, LLMD write failures may be seen under high load. The output of 'show security log llmd counters' can be used to view LLMD behaviour. PR1620018

- The flowd process might crash on SRX/NFX in AppQoE scenarios PR1621495
- The L2 switching doesn't work as expected when running VRRP on IRB interface PR1622680
- On SRX Series devices running DNS Security, if a DGA was detected and the action in the configuration was set to 'permit', under rare circumstances, a log would not be generated by the device. PR1624076
- In rare circumstances, PKID could crash and generate a core-file when there was limited memory available on the routing-engine PR1624613
- Coredumps might be reported on installing IDP security package PR1625364
- The flowd process lost heartbeat for 45 consecutive seconds without alarm raised PR1625579
- The error might be seen after configuring a unified security policy allowing some app categories PR1628202
- When viewing DNS Tunnel detections in the ATP Cloud portal, the Source-IP and Destination-IP metadata is reversed. PR1629995
- Depending on the configuration of the SRX, duplicate events may have been written to the on-box logging database. This fix improves LLMD performance by eliminating these duplicate write events PR1630123
- LLDP packets may be sent with incorrect source MAC for RETH/LAG child members PR1630886
- The srxpfe process might crash on SRX4600 PR1630990
- Reverse DNS Lookups will no longer be stored in the DNSF Cache when using DNS Security PR1631000
- Signature package update may fail and the appid process may crash on SRX devices PR1632205
- Tasks of download manager may not be resumed post reboot PR1633503
- On SRX Series devices running DNS Security, a dataplane memory leak may occur within the DNSF plugin when entries age-out of the DNSF cache PR1633519
- Most of the Dynamic Address Entries might report 0 IPv4 entries PR1634881
- The srxpfe process might crash while installing IDP sigpack with scaled traffic on SRX platforms PR1637181
- Unable to connect to domain controller on installing Microsoft KB update PR1637548
- The spcd process might crash during certain Linux based FPC card restart PR1638975
- The error is seen during the NON-ISSU upgrade from 15.1 to 18.2 and later releases PR1639610

- Configuration change during AppQoS session might result in PFE crash with flowd core PR1640768
- Traffic might be dropped due to the RX queue being full PR1641793
- The pfe crash may occur on JUNOS SRX platforms PR1642914
- The SKY ATP integrated service might get impacted on SRX with LSYS PR1643373
- On-Box Security Logs might be not storing the session-id as a 64-bit integer, resulting in incorrect session-id's being present in the on-box logs PR1644867
- 21.2R3 : Issue with the command "clear security idp counters packet-log logical-system all" PR1648187

Interfaces and Chassis

- Members mac might be different from parent reth0 interface, resulting loss of traffic PR1583702
- 21.4DCB SecPDT: SRX4600: dcd core at /.amd/svl-engdata5vs2/occamdev/build/freebsd/stable_12/20210819.161417__ci_fbsd_builder_stable_12.0.54769caa/src/lib/libc/i386/string/strncmp.S:69 PR1617881

Intrusion Detection and Prevention (IDP)

- 21.2R3:SRX345:vSRX3.0:Device is hanging while checking the cli " show security idp attack attack-list policy combine-policy" PR1616782

J-Web

- After a HA cluster is created, you are unable to edit it in J-Web PR1636237
- reboot/halt from J-web may fail on SRX series platforms PR1638370
- Significant performance improvements were made to JWeb in this release. PR1652676

Network Address Translation (NAT)

- DNS proxy service on SRX devices may stop working after commit operation is performed PR1598065
- New persistent NAT or normal source NAT sessions might fail due to noncleared aged out sessions PR1631815

Platform and Infrastructure

- The ppmd process might crash after an upgrade on SRX platforms PR1335526
- Error message "gencfg_cfg_msg_gen_handler drop" might be seen after running commit command PR1629647
- IP monitor may install default route with incorrect preference value when multiple IP monitoring is configured PR1634129
- SCB reset with Error : zfchip_scan line = 844 name = failed due to PIO errors PR1648850

Routing Protocols

- Observing commit error while configuring "routing-options rib inet6.0 static" on all Junos platforms PR1599273

Unified Threat Management (UTM)

- New UTM Content-Filtering CLI is changing from seclog to log PR1634580

User Interface and Configuration

- MGD core might be observed upon ISSU upgrade PR1632853

VPNs

- The configuration change in SRG-1 might cause HA link encryption tunnel flap PR1598338
- The process "iked" crash might be seen for IKEv1 based VPN tunnels PR1608724
- Uneven IPSEC tunnel distribution might be seen post tunnels re-establishment PR1615763
- Traffic over IPSec tunnels may be dropped post control link failure PR1627557
- Traffic loss over IPSEC tunnel might be seen on SRX platforms PR1628007
- SRX devices generates core dump after upgrading to any release PR1628947
- On all SRX products, when nat traversal is configured and working for an ipsec tunnel, there is a chance that the tunnel might stop processing packets after a rekey PR1636458
- The kmd process might crash if the IKE negotiation fragment packets are missed during initiating an IKE SA rekey PR1638437

Resolved Issues: 21.4R1

IN THIS SECTION

- Application Layer Gateways (ALGs) | 238
- Authentication and Access Control | 238
- Flow-Based and Packet-Based Processing | 238
- General Routing | 239
- Infrastructure | 241
- Interfaces and Chassis | 241
- Intrusion Detection and Prevention (IDP) | 241
- J-Web | 242
- Network Address Translation (NAT) | 242
- Platform and Infrastructure | 242
- Routing Policy and Firewall Filters | 243
- Routing Protocols | 243
- Unified Threat Management (UTM) | 243
- VPNs | 243

Application Layer Gateways (ALGs)

- ALG traffic might be dropped. PR1598017

Authentication and Access Control

- UAC authentication might not work post system reboot. PR1585158

Flow-Based and Packet-Based Processing

- Performance degradation might be observed when power-mode-ipsec is enabled. PR1599044
- The services offload packets processed counter not incremented in security flow statistics. PR1616875
- Security traffic log display service-name as none for some application. PR1619321

- Cleartext fragments are not processed by flow. PR1620803
- On SRX4600 and SRX5000 line of devices, when an interface is configured in TAP mode, the vlan-id-range is now supported in non-default routing instances. PR1624041

General Routing

- SSL-FP logging for non SNI session. PR1442391
- In non-FIPS mode, the RNG in FreeBSD 12 based Junos OS versions has been changed from the default FreeBSD Fortuna RNG to the FIPS/SP800-90A&B HMAC-DRBG CSPRNG. PR1529574
- Some transmitting packets might get dropped due to the disable-pfe action is not invoked when the fabric self-ping failure is detected. PR1558899
- The CLI command show pfe statistics traffic shows wrong output. PR1566065
- When using log templates with unified policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile set security log profile default-profile can be used to improve this behavior when multiple log profiles are defined. PR1570105
- Changes in SNMP traps configuration and data exported for TWAMP. PR1573169
- On SRX Series devices with Chassis Cluster, the tcp_timer_keep:Local(0x81100001:60753) Foreign(0x8f100001:33010) is seen in messages log every 80 seconds. PR1580667
- Traffic is dropped to or through VRRP virtual IP on SRX380 device. PR1581554
- The srxpfe process might stop on SRX1500 devices. PR1582989
- Secure Web proxy continue sending DNS query for unresolved DNS entry even after the entry was removed. PR1585542
- On SRX Series devices, significant performance improvements for JDPI's micro-application identification were included in this release. PR1585683
- The show security idp counters command is not having tenant command in the syntax. PR1586220
- IP packets might be dropped on SRX Series devices. PR1588627
- The jsqlsyncd process files generation might cause device to stop after upgrade. PR1589108
- The REST API does not work for SRX380 devices. PR1590810
- The issue (empty feed-name) starts with the hit returned from cache which points to the node with the parameter of feed-ID (2) inconsistent with the feeds-update (when it's 1). As a result the incorrect feed-ID points to the empty entry in the array of the feed-names. PR1591236

- J-Web deny log nested-application as UNKNOWN instead of specific application. PR1593560
- When combining log profiles and unified policies RT_FLOW_SESSION_DENY logs were not being generated corrected. PR1594587
- System logs are generated when maximum session or total memory limit is hit for packet capture. PR1594669
- The flowd process might stop when AppID marks the application as complete and the inspection limits are hit. PR1595310
- Node1 fpc0 (SPM) goes down after ISSU and RG0 failover. PR1595462
- Sometimes, when Jflow v9 flow record can contain wrong application id from cache, which can lead wrong identification of traffic application. PR1595787
- On SRX Series devices with SPC3, when SPC3 fails in specific circumstances, there might be delay observed in failover to other node. PR1596118
- The flowd process might generate core files if application services security policy is configured. PR1597111
- The srxpfe process might stop and generate a core file post "targeted-broadcast forward-only" interface-config commit. PR1597863
- The flowd process might generate core files if the AppQOS module receiving two packets of a session. PR1597875
- The flowd process might stop in AppQoE scenarios PR1599191
- The httpd-gk process generates core files when IPsec VPN is configured. PR1599398
- CRC or align errors and fragment frames might be seen with traffic against 400G ports. PR1601151
- Traffic might be dropped at NAT gateway if EIM is enabled. PR1601890
- Kernel crash might be seen when static routes are configured with GRE interfaces being used as next-hop. PR1601996
- The flowd process might stop if the DNS-inspection feature is enabled by configuring SMS policy. PR1604773
- Memory leak at the useridd process might be observed when integrated user firewall is configured. PR1605933
- When the tap mode is enabled, the packet on ge-0/0/0 is dropped on RX side. PR1606293
- The flowd process might stop if the DNS-inspection feature is enabled within SMS. PR1607251

- DNS proxy functionality might not work on VRRP interfaces. PR1607867
- Enabling dnsf traceoptions on SRX300 line of devices might result in flowd process to stop. PR1608669
- Enabling security-metadata-streaming-policy command might cause Packet Forwarding Engine stop. PR1610260
- DNS-based SecIntel statistics were not populating correctly on SRX Series devices. PR1611071
- On SRX Series devices running DNS security, the notification option 'log-detections' was not honoured. Prior to this release, a log was generated for every DNS request, regardless of its intent. PR1611177
- Interface might not come up when 10G port is connected to 1G SFP. PR1613475
- Enabling security-metadata-streaming DNS policy might cause a data plane memory leak. PR1613489
- On SRX Series devices running DNS Security in secure-wire mode, DGA verdicts would not be returned to the device. PR1616075
- The srxpfe process might stop when the DNS security feature is enabled. PR1616171
- Traffic might get dropped due to memory issue on some SRX Series devices. PR1620888
- Running DNS on all SRX Series devices, a memory leak on Packet Forwarding Engine might occur. PR1624655
- When viewing DNS Tunnel detections in the ATP Cloud portal, the Source-IP and Destination-IP metadata is reversed. PR1629995

Infrastructure

- Upgrade might fail when upgrading from previous releases. PR1602005

Interfaces and Chassis

- IPv4 or IPv6 address from the config on the interface might not be applied when the interface is moved from tenants to interface stanza in the configuration. PR1605250

Intrusion Detection and Prevention (IDP)

- IDP signature DB update fails. PR1594283
- Custom attack IDP policies might fail to compile. PR1598867

- IDP policy compilation is not happening when a commit check is issued prior to a commit. PR1599954
- The srxpfe process might stop while the IDP security package contains a new detector. PR1601380
- This release includes optimizations made to IDP that help improve its performance and behavior under load. PR1601926
- High Routing Engine CPU usage occurs when routing instance is configured under security idp security-package hierarchy level. PR1614013
- IDP signature install taking longer time. PR1615985
- Application identification DB update failing to download when used through IDP offline method. PR1623857

J-Web

- J-Web a custom application name contains "any" is listed under pre-defined applications. PR1597221
- J-Web might not display customer defined application services if one new policy is created. PR1599434
- J-Web application might stop and generate the httpd process core files. PR1602228
- Radius users might not be able to view or modify configuration through J-Web. PR1603993
- On all SRX Series devices, some widgets in J-Web might not load properly for logical systems users. PR1604929
- The error displays "your session has expired. click ok to re-login" when using root user. PR1611448
- The AM or PM time format is displayed in customize for last field at Monitor > Logs > All Events. PR1628649

Network Address Translation (NAT)

- Incorrect IPv6 UDP checksum inserted after translation of packet from IPv4 to IPv6. PR1596952

Platform and Infrastructure

- Junos OS: Upon receipt of specific sequences of genuine packets destined to the device the kernel will crash and restart (vmcore) (CVE-2021-0283, CVE-2021-0284). PR1595649
- The process mgd might stop with authentication setup. PR1600615

- SRX accounting and auditd process might not work on secondary node. PR1620564

Routing Policy and Firewall Filters

- High CPU usage might be seen on some SRX Series devices. PR1579425

Routing Protocols

- Short multicast packets drop using PIM when multicast traffic received at a non-RPT/SPT interface. PR1579452
- The fwauthd process generates core file when upgrading to Junos OS 21.2R1 release. PR1588393
- While testing pppoe_dhcpv6, observing commit error while configuring routing-options rib inet6.0 static. PR1599273

Unified Threat Management (UTM)

- There is no counter for juniper-local default action. PR1570500

VPNs

- The iked process might restart and generate core during session state activation or deactivation PR1573102
- The iked process might stop when IKEv2 negotiation fails on MX or SRX Series devices. PR1577484
- Memory leaks on the iked process on SRX5000 line of devices with SRX5K-SPC3 installed. PR1586324
- Certificate identifier length for PKI CMPv2 CA cert is not displayed as expected in certain cases. PR1589084
- The IPsec tunnel might not come up if configured with configuration payload in a certain scenario. PR1593408
- The kmd process might crash when VPN peer initiates using source-port other than 500. PR1596103
- Tail drops might occur on SRX Series devices if shaping-rate is configured on st-interface. PR1604039

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for SRX Series Gateways.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | **244**

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

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

For information about ISSU, see the Chassis Cluster User Guide for Security Devices.

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

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

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

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

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if

the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 8: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for vMX

IN THIS SECTION

- What's New | 246
- What's Changed | 247
- Known Limitations | 249
- Open Issues | 249
- Resolved Issues | 250
- Documentation Updates | 251
- Upgrade Instructions | 251

These release notes accompany Junos OS Release 21.4R2 for vMX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

- What's New in 21.4R2 | 246
- What's New in 21.4R1 | 246

Learn about new features introduced in this release for vMX Virtual Router.

What's New in 21.4R2

There are no new features or enhancements to existing features in Junos OS Release 21.4R2 for vMX.

What's New in 21.4R1

IN THIS SECTION

- Licensing | 246
- Operation, Administration, and Maintenance (OAM) | 247

Learn about new features introduced in this release for vMX Virtual Router.

Licensing

- **License renewal or automatic update (EX2300, EX3400, EX4300, EX4400-24MP, PTX10001-36MR, PTX10003, PTX10008, PTX10016, QFX5130-32CD, QFX5220, vMX, and vSRX)**—Starting in Junos OS Release 21.4R1, you can renew or automatically update all software feature licenses using the following commands:
  - `set system license autoupdate url <link>`
  - `set system license renew before-expiration <days>`

- `set system license renew interval <hours>`

The `license autoupdate` and `license renew` commands streamline license tracking. Use these commands to reduce the manual tracking effort for license renewal.

[See License Autoupdate and License Renew.]

Operation, Administration, and Maintenance (OAM)

- **Enhancements to Bidirectional Forwarding Detection (BFD)-triggered fast reroute (FRR) for unicast next hops and session-id-change-limiter-indirect (MX Series, PTX1000, PTX3000, PTX5000, PTX10001, PTX10002, PTX10016, QFX10002-60C, QFX10002, QFX10008, QFX10016, and vMX)** —In Junos OS Release 21.4R1, we've enhanced the BFD-triggered fast reroute (FRR) for unicast next hops and session-id-change-limiter-indirect to address the issue of traffic being silently discarded because of a session mismatch between the control plane and data plane.

  To limit the re-programming of the number of parent nodes of the indirect-nexthop and avoid additional the complexity in the Packet Forwarding Engine when the session-identifier id of the indirect nexthop is changed, use the `session-id-change-limiter-indirect` configuration statement at the `[edit routing-options]` hierarchy level.

  [See Bidirectional Forwarding Detection (BFD) for MPLS.]

What's Changed

IN THIS SECTION

- What's Changed in Release 21.4R2 | **248**
- What's Changed in Release 21.4R1 | **248**

Learn about what changed in this release for vMX Virtual Router.

What's Changed in Release 21.4R2

IN THIS SECTION

- Network Management and Monitoring | 248

Network Management and Monitoring

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

What's Changed in Release 21.4R1

IN THIS SECTION

- Network Management and Monitoring | 248

Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the

device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.

Known Limitations

There are no known limitations in hardware and software in Junos OS 21.4R2 for vMX Virtual Router.

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

Open Issues

IN THIS SECTION

- Platform and Infrstaructure | **249**

Learn about open issues in Junos OS Release 21.4R2 for vMX Virtual Router.

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

Platform and Infrstaructure

- In VMX platform, after a system reboot, the Protect-RE filter on lo0 interface is no longer applied. This issue has been fixed in 17.1R1 and later releases. A commit full can clear the issue. PR1604401

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.4R2 | 250
- Resolved Issues: 21.4R1 | 250

Learn about the issues fixed in this release for vMX Virtual Router.

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

Resolved Issues: 21.4R2

IN THIS SECTION

- Platform and Infrastructure | 250

Platform and Infrastructure

- AUTO-CORE-PR : JDI-RCT vRCT : vmxt_lnx core found @ topo_get_link jnh_features_get_jnh jnh_stream_attach PR1638166

Resolved Issues: 21.4R1

IN THIS SECTION

- Interfaces and Chassis | 250

Interfaces and Chassis

- Interface hold-time up does not work on vMX and MX150 devices. PR1604554

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for vMX Virtual Router.

Upgrade Instructions

You cannot upgrade Junos OS for the vMX router from earlier releases using the `request system software add` command.

You must deploy a new vMX instance using the downloaded software package.

Remember to prepare for upgrades with new license keys and/or deploying Agile License Manager.

Starting in Junos OS release 21.4R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

Junos OS Release Notes for vRR

IN THIS SECTION

- What's New | 252
- What's Changed | 252
- Known Limitations | 252
- Open Issues | 252
- Resolved Issues | 253
- Documentation Updates | 254

These release notes accompany Junos OS Release 21.4R2 for vRR. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features or enhancements to existing features in Junos OS Release 21.4R2 and 21.4R1 for Virtual Route Reflector.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R2 and 21.4R1 for Virtual Route Reflector.

Known Limitations

There are no known limitations in hardware and software in Junos OS 21.4R2 for Virtual Route Reflector.

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

To learn more about common BGP or routing known limitations in Junos OS 21.4R2, see "Known Limitations" on page 90 for MX Series routers.

Open Issues

There are no known issues in hardware and software in Junos OS Release 21.4R2 for Virtual Route Reflector.

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

To learn more about common BGP or routing knowns issues in Junos OS 21.4R2, see "Open Issues" on page 94 for MX Series routers.

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.4R2 | 253
- Resolved Issues: 21.4R1 | 253

Learn about the issues fixed in this release for Virtual Route Reflector.

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

Resolved Issues: 21.4R2

General Routing

- vRR: Support for flexible vlan-tagging on SR-IOV interfaces PR1541034
- The "monitor traffic interface" might not work for em2 on vRR/JRR200 PR1629242
- vRR VM might establish its identity as "Olive" after a CLI s/w upgrade PR1635950
- Video console for vRR might not work after an upgrade PR1644806

Resolved Issues: 21.4R1

IN THIS SECTION

- General Routing | 253

General Routing

- Memory might be exhausted when both the BGP rib-sharding and the BGP ORR (Optimal Route Reflection) enabled. PR1613104
- The process rpd might crash in BGP rib sharding scenario. PR1613723

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for Virtual Route Reflector.

Junos OS Release Notes for vSRX

IN THIS SECTION

- What's New | 254
- What's Changed | 258
- Known Limitations | 261
- Open Issues | 261
- Resolved Issues | 262
- Documentation Updates | 266
- Migration, Upgrade, and Downgrade Instructions | 267

These release notes accompany Junos OS Release 21.4R2 for vSRX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

- What's New in 21.4R2 | 255
- What's New in 21.4R1 | 255

Learn about new features introduced in this release for vSRX Virtual Firewall.

What's New in 21.4R2

There are no new features or enhancements to existing features in Junos OS Release 21.4R2 for vSRX Virtual Firewall.

What's New in 21.4R1

IN THIS SECTION

- Application Identification (AppID) | **255**
- Authentication and Access Control | **255**
- Flow-Based and Packet-Based Processing | **256**
- Interfaces | **256**
- Licensing | **256**
- Platform and Infrastructure | **257**
- Unified Threat Management (UTM) | **257**
- Additional Features | **258**

Learn about new features introduced in this release for vSRX Virtual Firewall.

Application Identification (AppID)

- **Dual stacking of IPv4 and IPv6 (SRX Series and vSRX)**—Starting in Junos OS Release 21.4R1, we support dual stacking of IPv4 and IPv6 addresses for overlay and underlay networks in an AppQoE configuration.
  [See Support for IPv6 Traffic in AppQoE.]

Authentication and Access Control

- **LDAP authentication for Juniper Secure Connect (SRX Series devices and vSRX with Juniper Secure Connect)**—In Junos OS Release 21.4R1, we've introduced support for native LDAP authentication with secure connection to simplify deployments of Juniper Secure Connect. With the LDAP authentication support, you can determine which groups should be granted access after successful authentication. Use the `address-assignment` option at the `[edit access profile profile-name authentication-order ldap ldap-options]` hierarchy level to assign IP addresses specifically for those groups of users to simplify IP address management.

[See ldap-options.]

Flow-Based and Packet-Based Processing

- **Support for MPLS Layer 3 VPN in flow mode (vSRX 3.0)** —Starting in Junos OS Release 21.4R1, we support MPLS Layer 3 VPN in flow mode. We also support IP unicast packet processing. Thus, IP unicast packets de-encapsulated from MPLS enter the flow processing when you enable `set security forwarding-options family mpls mode flow-based`.

  [See Flow Management in SRX Series Devices Using VRF Routing Instance.]

- **Support for fat flow (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 21.4R1, we support fat flow technology to improve the firewall and NAT throughput value up to 10 times of the current value.

  [See Understanding Symmetric Fat IPsec Tunnel.]

Interfaces

- **Microsoft Azure Advanced Networking with SR-IOV support (vSRX 3.0)**—Starting in Junos OS Release 21.4R1, vSRX 3.0 supports the Azure Accelerated Networking (AAN) feature. AAN utilizes the Mellanox single-root I/O virtualization (SR-IOV) virtual function for high-speed networking. Microsoft Azure uses Mellanox ConnectX-3, ConnectX-4, and ConnectX-5 NICs to support AAN. However, vSRX 3.0 supports only ConnectX-4 and ConnectX-5 AAN.

  See Understand vSRX with Microsoft Azure Cloud and Enable Accelerated Networking for Replicated VMs.

Licensing

- **License renewal or automatic update (EX2300, EX3400, EX4300, EX4400-24MP, PTX10001-36MR, PTX10003, PTX10008, PTX10016, QFX5130-32CD, QFX5220, vMX, and vSRX)**—Starting in Junos OS Release 21.4R1, you can renew or automatically update all software feature licenses using the following commands:

  - `set system license autoupdate url <link>`
  - `set system license renew before-expiration <days>`
  - `set system license renew interval <hours>`

  The `license autoupdate` and `license renew` commands streamline license tracking. Use these commands to reduce the manual tracking effort for license renewal.

  [See License Autoupdate and License Renew.]

Platform and Infrastructure

- **PKI usability enhancements (MX240, MX480, MX960, SRX Series, and vSRX)**—Starting in Junos OS Release 21.4R1, we've enhanced PKI commands to provide additional details about the local and certificate authority (CA)-issued certificates. With these enhancements, you can:

  - View the CA certificate status of a CA profile group using the `request security pki ca-profile-group-status ca-group-name` *`group-name`* command. See request security pki ca-profile-group-status.

  - Configure certificate automatic reenrollment trigger time in days, hours, or percentage using the `set security pki auto-re-enrollment cmpv2 certificate-id certificate-id-name re-enroll-time (days` *`value`*`| hours` *`value`*`| percentage` *`value`*`)` or `set security pki auto-re-enrollment scep certificate-id certificate-id-name re-enroll-time (days` *`value`*`| hours` *`value`*`| percentage` *`value`*`)` command. See auto-re-enrollment.

  - View the CA chain, SHA256 fingerprint, and certificate serial number (hexadecimal and decimal format) for a local certificate using the `show security pki local certificate <`*`cert_id`*`> detail` command. See show security pki local-certificate (View).

  - View the CA profile associated with a CA certificate and SHA256 fingerprint using the `show security pki ca-certificate <brief|detail>` command. See show security pki ca-certificate (View).

  - View additional verification information about local and CA certificate using the `request security pki local-certificate verify` and the `request security pki ca-certificate verify` command, respectively. See request security pki ca-certificate verify (Security) and request security pki local-certificate verify (Security).

  - View more PKI-related statistics using the `show security pki statistics` command. Clear the PKI statistics using the `clear security pki statistics` command. See show security pki statistics and clear security pki statistics.

Unified Threat Management (UTM)

- **Content filtering based on file content (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 21.4R1, content security (UTM) performs content filtering to determine the file type based on the file content and not on file extensions. The file content is first analyzed to accurately determine the file type.

  This feature replaces the legacy content filtering based on MIME type, content type, and protocol commands.

  You can define the content filtering rule-set and rules from the `[edit security utm utm-policy <utm-policy-name> content-filtering]` hierarchy and use these rules from the `[edit security utm default-configuration content-filtering]` hierarchy for controlling the traffic direction.

  The existing `show security utm content-filtering statistics` command is enhanced to display the content filtering system statistics and errors.

[See Content Filtering, content-filtering (Security UTM Policy), utm, and utm default-configurationshow security utm content-filtering statistics.]

Additional Features

We've extended support for the following features to these platforms.

- **Configure concurrent connections** (SRX Series devices and vSRX running iked). Configure the number of concurrent connections that the group profile supports using the `connections-limit` configuration statement at the `[edit security ike gateway gateway-name dynamic]` hierarchy level. We support this configuration for both IKEv1 and IKEv2. This configuration is applicable only to AutoVPN, ADVPN, dynamic endpoint, and remote access (preshared-key and PKI-based tunnels).

  There are no restrictions on the number of connections accepted if you haven't configured the `connections-limit` option.

  [See dynamic (Security)].

- **Dynamic routing protocols** (MX240, MX480, and MX960 with MX-SPC3, SRX5000 line of devices with SPC3 card and vSRX running iked). We support the exchange of dynamic routing information through IPsec VPN tunnels. You can now enable the dynamic routing protocol, such as OSPF, BGP, BFD, PIM, and RIP on a st0 interface of an IPsec VPN tunnel.

  This feature is supported only if the `junos-ike` package is installed in your device.

  [See Routing Protocols Support on IPsec VPN Tunnels.]

What's Changed

IN THIS SECTION

- What's Changed in Release 21.4R2 | **259**
- What's Changed in Release 21.4R1 | **260**

Learn about what changed in this release for vSRX Virtual Firewall.

What's Changed in Release 21.4R2

IN THIS SECTION

- Network Management and Monitoring | 259
- Platform and Infrastructure | 259
- Unified Threat Management (UTM) | 260

Learn about what changed in this release for vSRX.

Network Management and Monitoring

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

Platform and Infrastructure

Instance Types on AWS platform (vSRX and vSRX 3.0)—Starting with Junos OS release 21.4R2, only C5 instance types are supported on AWS platform. C4 instance type with vSRX is deprecated. If you wish to upgrade the Junos OS on a C4 vSRX instance, then you must deploy a new vSRX instance using the supported instance types. See Interface Mapping for vSRX on AWS.

Unified Threat Management (UTM)

- **Content filtering CLI updates (SRX Series and vSRX)**—We've the following updates to the content filtering CLI:

  - Trimmed the list of file types supported for content filtering rule match criteria. Instead of uniquely representing different variants of a file type, now only one `file-type` string represents all variants. Hence, the `show security utm content-filtering statistics` output is also updated to align with the new file types available in the rule match criteria.

  - Renamed the content filtering security logging option `seclog` to `log` to match with the Junos OS configuration standard.

  - Rephrased the `reason` string associated with content filtering security log message.

  [See content-filtering (Security UTM Policy), content-filtering (Security Feature Profile), and show security utm content-filtering statistics.]

What's Changed in Release 21.4R1

IN THIS SECTION

- Network Management and Monitoring | **260**
- Platform and Infrastructure | **260**

Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.

Platform and Infrastructure

- The advanced anti-malware Hash feature is deprecated. PR1604426

Known Limitations

IN THIS SECTION

- Platform and Infrastructure | 261

Learn about known limitations in Junos OS Release 21.4R2 for vSRX Virtual Firewall.

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

Platform and Infrastructure

- From Junos OS release 21.4R2 onwards, the supported AWS instance types are C5 and C6. Instance type C4 support with vSRX is deprecated. If you wish to upgrade the Junos OS on a C4 vSRX instance, then you must deploy a new vSRX instance using the supported instance types. See Launch a vSRX Instance on an Amazon Virtual Private Cloud.
- There is max limit on number of vlans that can be configured per VF for i40e driver. The number is 8. The maximum VLAN supported per VF is 63 VLANs in SR-IOV trust mode. PR1610282
- When multiple vlan-tagging sub-interfaces are configured and switching vSRX3.0 between vlan-tagging and flexible-vlan-tagging support mode, traffic will stop and must reboot vSRX3.0 to recover, if trust mode is disabled for the virtual functions. PR1610287

Open Issues

Learn about open issues in Junos OS Release 21.4R2 for vSRX Virtual Firewall.

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

Flow-Based and Packet-Based Processing

- Traffic in the power mode still passthrough when the ingress logic interface is manually disabled. PR1604144

- The ICMPv6 TCP sequence information is missing in the ICMP v6 error generated. PR1611202
- You must keep 1 to 2 minutes gap between two configuration commits if there are lots of security policies which need time to be processed. PR1625531

Platform and Infrastructure

- With ssl-proxy configured along with web-proxy, the client session might not closed on the device even though proxy session ends gracefully. PR1580526
- The prerformance will be improved by set security forwarding-options no-allow-dataplane-sleep command. PR1602564
- One needs to configure set security forwarding-options no-allow-dataplane-sleep for high traffic rate use cases. PR1602606
- AMR first session traffic is not copying over multiple paths for IPv6 traffic over IPv6 IPsec tunnel mode PR1643570

Routing Policy and Firewall Filters

- Policy re-match is not working when source-tenant or destination-service match criteria modified. PR1625172

VPNs

- When using Group VPN, in certain cases, the PUSH ACK message from the group member to the group key server may be lost. The group member can still send rekey requests for the TEK SAs before the hard lifetime expiry. Only if the key server sends any new PUSH messages to the group members, those updates would not be received by the group member since the key server would have removed the member from registered members list. PR1608290

Resolved Issues

IN THIS SECTION

- Resolved Issues: 21.4R2 | **263**
- Resolved Issues: 21.4R1 | **264**

Learn about the issues fixed in this release for vSRX Virtual Firewall.

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

Resolved Issues: 21.4R2

Flow-Based and Packet-Based Processing

- On SRX-Series devices using Unified Policies with IPv6, when attempting to reject certain dynamic-applications a flowd core could be generated PR1601806

General Routing

- SRX_RIAD:CSRX:LOG: RT-Log pattern is not matching in 21.1R1, 21.2R2, 21.2R1 and 21.4R1. PR1565153
- PKID core during auto-re-enrollment of CMPv2 certificates. PR1580442
- 20.1R3:SRX-RIAD:vSRX3.0: Web-proxy: Getting UNKNOWN instead of HTTP-PROXY for application and UNKNOWN instead of GOOGLE-GEN in RT-FLOW close messages PR1588139
- During SaaS probing, due to race condition between APP entry addition and session processing, this core is seen. PR1622787
- On SRX Series devices running DNS Security, if a DGA was detected and the action in the configuration was set to 'permit', under rare circumstances, a log would not be generated by the device. PR1624076
- The application package installation might fail with error in SRX platforms PR1626589
- vSRX3 on VMware ESXi versions 7.0u2 or 7.0u3 with i40e SR-IOV: Traffic stopped after reboot PR1627481
- vSRX: "Resource errors" in "show interfaces extensive" PR1629986
- Signature package update may fail and the appid process may crash on SRX devices PR1632205
- On SRX Series devices running DNS Security, a dataplane memory leak may occur within the DNSF plugin when entries age-out of the DNSF cache PR1633519
- Application group name is not found for micro apps in CLI show output PR1640040
- The pfe crash may occur on JUNOS SRX platforms PR1642914

Infrastructure

- The failover process may become slow in a vSRX cluster if the gstatd daemon stops running PR1626423

Intrusion Detection and Prevention (IDP)

- 21.2R3:SRX345:vSRX3.0:Device is hanging while checking the cli " show security idp attack attack-list policy combine-policy" PR1616782

J-Web

- J-Web may only allow certain types of interfaces to be added in a routing-instance PR1637917
- Significant performance improvements were made to JWeb in this release. PR1652676

Routing Protocols

- Memory leak in 'global data shm' process might lead to traffic outage PR1626704

Unified Threat Management (UTM)

- New UTM Content-Filtering CLI is changing from seclog to log PR1634580
- Web browser traffic might get blocked when matched to the content-filtering rule with file-types 7z PR1656266

VPNs

- The process kmd might crash if the ike gateway is configured with two ip-address PR1626830
- Issue in Certificate-based VPN tunnels initiation while using GCP KMS PR1628722
- On all SRX products, when nat traversal is configured and working for an ipsec tunnel, there is a chance that the tunnel might stop processing packets after a rekey PR1636458

Resolved Issues: 21.4R1

IN THIS SECTION

Application Layer Gateways (ALGs) | 265

- Authentication and Access Control | 265
- General Routing | 265
- Intrusion Detection and Prevention (IDP) | 266
- Network Address Translation (NAT) | 266
- Routing Policy and Firewall Filters | 266
- Routing Protocols | 266
- VPNs | 266

Application Layer Gateways (ALGs)

- ALG traffic might be dropped. PR1598017

Authentication and Access Control

- UAC authentication might not work post system reboot. PR1585158

General Routing

- IKE configure mode payload is not pushing secondary DNS and secondary WINS attributes to Xauth module with IKEv1. Hence, the client is not getting assigned with secondary DNS and secondary WINS with IKEv1. PR1558831
- When using log templates with unified policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile (set security log profile default-profile) that can be used to improve this behavior when multiple log profiles are defined. PR1570105
- The srxpfe or flowd process might stop when using Juniper ATP cloud. PR1573157
- vSRX unreachable over SSH after integration with KMS on AWS. PR1584415
- When combining log profiles and unified policies RT_FLOW_SESSION_DENY logs were not being generated corrected. PR1594587
- Network based application recognition value for IPv4 application ID are not as expected. PR1595787
- The FPC might not come up if the vCPU number is configured more than 5 vCPU on vSRX3.0. PR1601823
- vSRX3.0 with Mellanox SR-IOV interfaces on VMware, the interface order is random. PR1604060

- vSRX might stop forwarding traffic 60 days after Junos OS upgrade due to the trial license expiring. PR1609551
- For apps getting classified on first packet, the volume update syslog is not getting generated. PR1613516
- The interface speed is limited to 1G on vSRX 2.0 even the speed is set as more than 1G. PR1617397
- Assert core might be seen when the application goes to **no path selected** state. PR1617506
- Running DNS on all SRX Series devices, a memory leak on Packet Forwarding Engine might occur. PR1624655

Intrusion Detection and Prevention (IDP)

- The flowd or srxpfe process might stop when IDP is used on Junos OS Release 21.2R1. PR1610706

Network Address Translation (NAT)

- SNMP object "jnxJsNatSrcNumPortAvail" does not show the proper value. PR1611479

Routing Policy and Firewall Filters

- After policy configuration commit with source tenant and destination services id field set as 0 due to this Incoming traffic processed by first policy. PR1617026
- Policy re-match extensive is not working for SVR traffic. PR1618717

Routing Protocols

- The rpd process generates core files because of memory corruption. PR1599751

VPNs

- Unable to set DynamoDB in HSM module. PR1599069

Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R2 and 21.4R1 for vSRX Virtual Firewall.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 273

This section contains information about how to upgrade Junos OS for vSRX using the CLI. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

You also can upgrade to Junos OS Release 21.4R1 for vSRX using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS.

Direct upgrade of vSRX from Junos OS 15.1X49 Releases to Junos OS Releases 17.4, 18.1, 18.2, 18.3,18.4, 19.1, 19.2 and 19.4 is supported.

The following limitations apply:

- Direct upgrade of vSRX from Junos OS 15.1X49 Releases to Junos OS Release 19.3 and higher is not supported. For upgrade between other combinations of Junos OS Releases in vSRX and vSRX 3.0, the general Junos OS upgrade policy applies.
- The file system mounted on /var usage must be below 14% of capacity.

  Check this using the following command:

  ```
  show system storage | match " /var$" /dev/vtbd1s1f
   2.7G        82M       2.4G         3%  /var
  ```

  Using the `request system storage cleanup` command might help reach that percentage.
- The Junos OS upgrade image must be placed in the directory /var/host-mnt/var/tmp/. Use the `request system software add /var/host-mnt/var/tmp/<upgrade_image>`
- We recommend that you deploy a new vSRX virtual machine (VM) instead of performing a Junos OS upgrade. That also gives you the option to move from vSRX to the newer and more recommended vSRX 3.0.

- Ensure to back up valuable items such as configurations, license-keys, certificates, and other files that you would like to keep.

NOTE: For ESXi deployments, the firmware upgrade from Junos OS Release 15.1X49-Dxx to Junos OS releases 17.x, 18.x, or 19.x is not recommended if there are more than three network adapters on the 15.1X49-Dxx vSRX instance. If there are more than three network adapters and you want to upgrade, then we recommend that you either delete all the additional network adapters and add the network adapters after the upgrade or deploy a new vSRX instance on the targeted OS version.

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 21.4R1 for vSRX .tgz** file from the Juniper Networks website. Note the size of the software image.
2. Verify that you have enough free disk space on the vSRX instance to upload the new software image.

```
root@vsrx> show system storage
       Filesystem              Size       Used      Avail  Capacity   Mounted on
       /dev/vtbd0s1a           694M       433M       206M       68%  /
       devfs                   1.0K       1.0K         0B      100%  /dev
       /dev/md0                1.3G       1.3G         0B      100%  /junos
       /cf                     694M       433M       206M       68%  /junos/cf
       devfs                   1.0K       1.0K         0B      100%  /junos/dev/
       procfs                  4.0K       4.0K         0B      100%  /proc
       /dev/vtbd1s1e           302M        22K       278M        0%  /config
       /dev/vtbd1s1f           2.7G        69M       2.4G        3%  /var
       /dev/vtbd3s2             91M       782K        91M        1%  /var/host
       /dev/md1                302M       1.9M       276M        1%  /mfs
       /var/jail               2.7G        69M       2.4G        3%  /jail/var
       /var/jails/rest-api       2.7G        69M       2.4G      3%  /web-api/var
       /var/log                2.7G        69M       2.4G        3%  /jail/var/log
       devfs                   1.0K       1.0K         0B      100%  /jail/dev
       192.168.1.1:/var/tmp/corefiles       4.5G       125M       4.1G    3%  /var/crash/
corefiles
       192.168.1.1:/var/volatile       1.9G       4.0K       1.9G    0%  /var/log/host
       192.168.1.1:/var/log       4.5G       125M       4.1G     3%  /var/log/hostlogs
```

```
        192.168.1.1:/var/traffic-log       4.5G       125M       4.1G    3%  /var/traffic-log
        192.168.1.1:/var/local       4.5G       125M       4.1G    3%  /var/db/host
        192.168.1.1:/var/db/aamwd       4.5G       125M       4.1G    3%  /var/db/aamwd
        192.168.1.1:/var/db/secinteld       4.5G       125M       4.1G    3%  /var/db/secinteld
```

3. Optionally, free up more disk space, if needed, to upload the image.

```
root@vsrx> request system storage cleanup
       List of files to delete:
       Size Date       Name
       11B Sep 25 14:15 /var/jail/tmp/alarmd.ts
       259.7K Sep 25 14:11 /var/log/hostlogs/vjunos0.log.1.gz
       494B Sep 25 14:15 /var/log/interactive-commands.0.gz
       21.4K Sep 25 14:15 /var/log/messages.0.gz
       27B Sep 25 14:15 /var/log/wtmp.0.gz
       27B Sep 25 14:14 /var/log/wtmp.1.gz
       3027B Sep 25 14:13 /var/tmp/BSD.var.dist
       0B Sep 25 14:14 /var/tmp/LOCK_FILE
       666B Sep 25 14:14 /var/tmp/appidd_trace_debug
       0B Sep 25 14:14 /var/tmp/eedebug_bin_file
       34B Sep 25 14:14 /var/tmp/gksdchk.log
       46B Sep 25 14:14 /var/tmp/kmdchk.log
       57B Sep 25 14:14 /var/tmp/krt_rpf_filter.txt
       42B Sep 25 14:13 /var/tmp/pfe_debug_commands
       0B Sep 25 14:14 /var/tmp/pkg_cleanup.log.err
       30B Sep 25 14:14 /var/tmp/policy_status
       0B Sep 25 14:14 /var/tmp/rtsdb/if-rtsdb
       Delete these files ? [yes,no] (no) yes
<
output omitted>
```

NOTE: If this command does not free up enough disk space, see [SRX] Common and safe files to remove in order to increase available system storage for details on safe files you can manually remove from vSRX to free up disk space.

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 21.4R1 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE.tgz /var/crash/corefiles/
```

5. From operational mode, install the software upgrade package.

```
root@vsrx> request system software add /var/crash/corefiles/junos-vsrx-
x86-64-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE signed by
PackageDevelopmentEc_2021 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 21.4 software.
WARNING:     It will save JUNOS configuration files, and SSH keys
WARNING:     (if configured), but erase all other files and information
WARNING:     stored on this machine.  It will attempt to preserve dumps
WARNING:     and log files, but this can not be guaranteed.  This is the
WARNING:     pre-installation stage and all the software is loaded when
WARNING:     you reboot the system.
Saving the config files ...
Pushing Junos image package to the host...
Installing /var/tmp/install-media-srx-mr-vsrx-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE-linux.tgz
Setting up Junos host applications for installation ...
============================================
Host OS upgrade is FORCED
Current Host OS version: 3.0.4
New Host OS version: 3.0.4
Min host OS version required for applications: 0.2.4
============================================
Installing Host OS ...
upgrade_platform: --------------------
upgrade_platform: Parameters passed:
upgrade_platform: silent=0
upgrade_platform: package=/var/tmp/junos-srx-mr-vsrx-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE-
```

```
linux.tgz
upgrade_platform: clean install=0
upgrade_platform: clean upgrade=0
upgrade_platform: Need reboot after staging=0
upgrade_platform: --------------------
upgrade_platform:
upgrade_platform: Checking input /var/tmp/junos-srx-mr-
vsrx-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE-linux.tgz is valid.
upgrade_platform: Backing up boot assets..
cp: omitting directory '.'
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
initrd.cpio.gz: OK
upgrade_platform: Checksum verified and OK...
/boot
upgrade_platform: Backup completed
upgrade_platform: Staging the upgrade package - /var/tmp/junos-srx-mr-
vsrx-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE-linux.tgz..
./
./bzImage-intel-x86-64.bin
./initramfs.cpio.gz
./upgrade_platform
./HOST_COMPAT_VERSION
./version.txt
./initrd.cpio.gz
./linux.checksum
./host-version
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
upgrade_platform: Checksum verified and OK...
upgrade_platform: Staging of /var/tmp/junos-srx-mr-
vsrx-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE-linux.tgz completed
upgrade_platform: System need *REBOOT* to complete the upgrade
upgrade_platform: Run upgrade_platform with option -r | --rollback to rollback the upgrade
Host OS upgrade staged. Reboot the system to complete installation!
WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software rollback'
```

```
WARNING:     command as soon as this operation completes.
NOTICE: 'pending' set will be activated at next reboot...
Rebooting. Please wait ...
shutdown: [pid 13050]
Shutdown NOW!
*** FINAL System shutdown message from root@ ***
System going down IMMEDIATELY
Shutdown NOW!
System shutdown time has arrived\x07\x07
```

If no errors occur, Junos OS reboots automatically to complete the upgrade process. You have successfully upgraded to Junos OS Release 21.4R1 for vSRX.

NOTE: Starting in Junos OS Release 17.4R1, upon completion of the vSRX image upgrade, the original image is removed by default as part of the upgrade process.

6. Log in and use the `show version` command to verify the upgrade.

```
--- JUNOS 21.4-2021-10-12.0_RELEASE_21.4_THROTTLE Kernel 64-bit
JNPR-11.0-20211012.170745_fbsd-
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ # cli
root> show version
Model: vsrx
Junos: 21.4-2021-10-12.0_RELEASE_21.4_THROTTLE
JUNOS OS Kernel 64-bit  [20211012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20211012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20211012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20211012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20211012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20211012.170745_fbsd-builder_stable_11]
JUNOS py extensions [20211017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20211017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20211012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20211012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20211017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20211017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20211017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20211017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20211017.110007_ssd-builder_release_174_throttle]
```

```
JUNOS srx libs compat32 [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20211017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20211017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20211017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20211017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20211017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20211017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20211012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20211017.110007_ssd-builder_release_174_throttle]
```

Validating the OVA Image

If you have downloaded a vSRX .ova image and need to validate it, see Validating the vSRX .ova File for VMware.

Note that only .ova (VMware platform) vSRX images can be validated. The .qcow2 vSRX images for use with KVM cannot be validated the same way. File checksums for all software images are, however, available on the download page.

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

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

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

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

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases.

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

Table 9: EOL and EEOL Releases

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

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

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Licensing

In 2020, Juniper Networks introduced a new software licensing model. The Juniper Flex Program comprises a framework, a set of policies, and various tools that help unify and thereby simplify the multiple product-driven licensing and packaging approaches that Juniper Networks has developed over the past several years.

The major components of the framework are:

- A focus on customer segments (enterprise, service provider, and cloud) and use cases for Juniper Networks hardware and software products.
- The introduction of a common three-tiered model (standard, advanced, and premium) for all Juniper Networks software products.
- The introduction of subscription licenses and subscription portability for all Juniper Networks products, including Junos OS and Contrail.

For information about the list of supported products, see Juniper Flex Program.

Finding More Information

- **Feature Explorer**—Juniper Networks Feature Explorer helps you to explore software feature information to find the right software release and product for your network.

  https://apps.juniper.net/feature-explorer/

- **PR Search Tool**—Keep track of the latest and additional information about Junos OS open defects and issues resolved.

  https://prsearch.juniper.net/InfoCenter/index?page=prsearch

- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms.

  https://apps.juniper.net/hct/home

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

- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6.

  https://pathfinder.juniper.net/compliance/

Requesting Technical Support

IN THIS SECTION

- Self-Help Online Tools and Resources | **276**
- Creating a Service Request with JTAC | **277**

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at https://www.juniper.net/content/dam/www/assets/resource-guides/us/en/jtac-user-guide.pdf.
- Product warranties—For product warranty information, visit https://support.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://support.juniper.net/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://supportportal.juniper.net/s/knowledge
- Download the latest versions of software and review release notes: https://support.juniper.net/support/downloads/
- Search technical bulletins for relevant hardware and software notifications: https://supportportal.juniper.net/s/knowledge
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://supportportal.juniper.net/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://support.juniper.net/support/requesting-support/
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

Revision History

24 November 2023—Revision 14, Junos OS Release 21.4R2– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

10 August 2023—Revision 13, Junos OS Release 21.4R2– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

20 July 2023—Revision 12, Junos OS Release 21.4R2– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

4 May 2023—Revision 11, Junos OS Release 21.4R2– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

9 September 2022—Revision 10, Junos OS Release 21.4R2– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

29 July 2022—Revision 9, Junos OS Release 21.4R2– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

17 May 2022—Revision 8, Junos OS Release 21.4R2– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

14 April 2022—Revision 7, Junos OS Release 21.4R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

3 March 2022—Revision 6, Junos OS Release 21.4R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

17 February 2022—Revision 5, Junos OS Release 21.4R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

20 January 2022—Revision 4, Junos OS Release 21.4R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

13 January 2022—Revision 3, Junos OS Release 21.4R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

28 December 2021—Revision 2, Junos OS Release 21.4R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

16 December 2021—Revision 1, Junos OS Release 21.4R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.