Release Notes

Published
2022-07-29

Junos OS Release 21.2R1 for the 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®

KEY FEATURES

- Use this video to take a quick look at some of the key features introduced in Junos OS Release 21.2R1.
- Refer to Key Features in Junos OS Release 21.2 to quickly learn about the most important Junos OS features and how you can deploy them in your network.

SOFTWARE HIGHLIGHTS

- AutoVPN PSK support (SRX5000 line of devices with SPC3 card and vSRX)
- Display dynamic-applications and URL category hit counts in a security policy (NFX Series and SRX Series) cSRX support on AWS (cSRX)
- DNS DGA and tunnel detection
- End-of-message notification for Routing Engine sensors (EX2300, EX4300, EX4300-MP, EX9200, MX240, MX960, MX10016, MX2010, MX2020, PTX1000, PTX3000, PTX10001, QFX5100, QFX5110, QFX5120, and QFX10002)
- Mellanox support (vSRX 3.0)
- Optimized inter-subnet multicast support with symmetric bridge domain configuration in an EVPN-VXLAN fabric (QFX5110, QFX5120, QFX10002-36Q, and QFX10002-72Q)
- Enhanced CFM support (ACX5448, ACX5448-M, and ACX5448-D)
- Enhancements to prefix-limit and accepted-prefix-limit configuration statements, and updates to show bgp neighbor command (ACX1000, EX9200, MX Series, PTX5000, and QFX10002)
- TCP proxy short-circuit (SRX Series)

- Juniper Agile Licensing (EX2300, EX3400, EX4300, and EX4400)
- Junos Multi-Access User Plane support for 5G user plane function (MX204, MX240, MX480, MX960, and MX10003)
- RSVP-TE supports preempting secondary LSPs that are signaled but not active (MX Series and PTX Series)
- Unified policy support for firewall user authentication (SRX Series and vSRX)
- Secure packet capture to cloud (EX4400)
- G.8275.1 Telecom profile and PTP over Ethernet encapsulation support (ACX2100 and ACX2200)
- Hardware-assisted inline BFD (QFX5120-32C and QFX5120-48Y)
- Interoperability of MPC10E with MX-SPC3 for IPSec services steering (MX240, MX480, and MX960)
- Interoperability of MPC10E with MX-SPC3 to support TLB (MX240, MX480, and MX960)
- Support for BGP MVPN (ACX710 routers)
- Increased memory allocation for Junos VM (MX204)
- TLS version 1.3 support for SSL proxy (SRX Series)

Day One+

- Use this guide to get your Junos OS up and running in three quick steps.

Table of Contents

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 21.2R1 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.

Key Features in Junos OS Release 21.2

Use this video to take a quick look at some of the key features introduced in Junos OS Release 21.2R1.

Here is the list of all key features in this release. For more information about a feature, click the link in the feature description.

- **DNS DGA and tunnel detection (SRX Series)**—Starting in Junos OS Release 21.2R1, you can configure DNS Domain Generation Algorithm (DGA) detection and DNS tunnel detection. This feature enables you to block the malicious domains and DNS-tunneled requests or responses generated by infected hosts and command-and-control (C&C) servers. DGA periodically generates a large number of domain names that are used as rendezvous points (RPs) with their C&C servers. DNS tunneling is a cyberattack method that encodes the data of malicious programs or protocols in DNS queries and responses.

  Use the `set security-metadata-streaming policy` *`policy-name`* `detections dga` and `set security-metadata-streaming policy` *`policy-name`* `detections tunneling` commands at the `[edit services]` hierarchy to configure DNS DGA and tunneling detections.

  [See security-metadata-streaming.]

- **End-of-message notification for Routing Engine sensors (EX2300, EX4300, EX4300-MP, EX9200, MX240, MX960, MX10016, MX2010, MX2020, PTX1000, PTX3000, PTX10001, QFX5100, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we've introduced an end-of-message (EoM) Boolean flag for all Junos telemetry interface (JTI) Routing Engine sensors. The flag notifies the collector that the current wrap has completed for a particular sensor path. A wrap is a complete key-value data dump for all the leaves under a sensor path.

The EoM flag also enables the collector to detect when the end of wrap occurs without having to compare stream creation timestamp values that the collector receives from the packets. Comparing timestamp values is costly time-wise and delays data aggregation.

To use this feature with gRPC Network Management Interface (gNMI) transport or Remote Procedure Call (gRPC), retrieve the protobuf files from the relevant branch on the Juniper Networks download site:

- GnmiJuniperTelemetryHeaderExtension.proto (gNMI)
- agent.proto (for gRPC)

For example: https://github.com/Juniper/telemetry/blob/master/20.3/20.3R1/protos/GnmiJuniperTelemetryHeaderExtension.proto.

After you download and install the new protobuf files on a collector, the EoM field is present in the packets received.

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

- **Optimized inter-subnet multicast support with symmetric bridge domain configuration in an EVPN-VXLAN fabric (QFX5110, QFX5120, QFX10002-36Q, and QFX10002-72Q)**—Starting in Junos OS Release 21.2R1, you can configure optimized inter-subnet multicast (OISM) on leaf devices and border leaf devices in an EVPN-VXLAN edge-routed bridging overlay fabric. This feature helps optimize the routing of multicast traffic across VLANs in an EVPN tenant domain. This feature uses a supplemental bridge domain (SBD) and a multicast VLAN (MVLAN) to route multicast traffic from or to devices outside of the fabric. This feature also works with existing IGMP snooping and selective multicast (SMET) forwarding optimizations to minimize replication in the EVPN core when bridging within tenant VLANs.

  With this implementation, you must enable OISM and IGMP snooping on all the leaf and border leaf devices in the EVPN-VXLAN fabric. You also must configure the SBD and all tenant VLANs symmetrically on all leaf and border leaf devices in the fabric.

  You can use OISM with:

  - EVPN on the `default-switch` instance with VLAN-aware bundle service model (Layer 2)
  - Routing instances of type `vrf` (Layer 3)
  - EVPN single-homing or multihoming (all-active mode)
  - IGMPv2
  - Multicast sources and receivers within the EVPN data center
  - Multicast sources and receivers outside the EVPN data center that are reachable through the border leaf devices

[See Optimized Inter-Subnet Multicast in EVPN Networks.]

- **Enhanced CFM support (ACX5448, ACX5448-M, and ACX5448-D)**—Starting in Junos OS Release 21.2R1, you can enable the performance monitoring responder functionality without enabling the transmission of continuity check messages (CCM). To enable the performance monitoring responder functionality without enabling CCM transmission, configure our new configuration statement `send-zero-interval-ccm` under the `[edit protocols protocols oam ethernet connectivity-fault-management]` hierarchy level. After you configure the statement, if the continuity-check is not enabled, CCMs are not transmitted, but are programmed to receive the CFM packets for that maintenance endpoint (MEP) level.

  [See IEEE 802.1ag OAM Connectivity Fault Management Overview and connectivity-fault-management (EX Series Switch Only).]

- **Juniper Agile Licensing (EX2300, EX3400, EX4300, and EX4400)**—Starting in Junos OS Release 21.2R1, the listed EX Series switches support Juniper Agile Licensing.

  Juniper Agile Licensing provides simplified and centralized license administration and deployment. You can use Juniper Agile Licensing to install and manage licenses for hardware and software features.

  Juniper Agile Licensing supports soft enforcement and hard enforcement of hardware and software feature licenses.

  - With soft enforcement, if you configure a feature without a license, Junos OS displays a warning when you commit the configuration. However, the feature remains operational. In addition, Junos OS generates periodic alarms indicating that you need the license to use the feature. You can see the list of alarms at System Log Explorer.

  - With hard enforcement, if you configure a feature without a license, Junos OS displays a warning when you commit the configuration. The feature is not operational until the license is installed. In addition, Junos OS generates periodic syslog messages indicating that you need the license to use the feature. You can see the list of syslog messages at System Log Explorer.

  Table 1 on page 4 describes the licensing support for soft-enforced features on EX2300 switches.

Table 1: Licensed Features on EX2300 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operation, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis*

Table 1: Licensed Features on EX2300 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRP version 3 • Multicast Source Discovery protocol (MSDP) • OAM and Maintenance CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • VRRP

Virtual Chassis*—We've included Virtual Chassis license in the Standard license model on EX2300-C 12-port switches. However, we don't include the Virtual Chassis license on EX2300 24-port and 48-port switch models. You need to purchase the license separately.

Table 2 on page 6 describes the licensing support for soft-enforced features on EX3400 switches.

Table 2: Licensed Features on EX3400 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 2: Licensed Features on EX3400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRP version 3, and virtual router support for unicast • Filter-based forwarding (FBF) • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 2: Licensed Features on EX3400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Premium	Campus and access Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRPv3, virtual router support for unicast, and FBF • Multicast Source Discovery Protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP • BGP and multiprotocol BGP (MBGP) • IS-IS

Table 3 on page 9 describes the licensing support for soft-enforced features on EX4300 switches.

Table 3: Licensed Features on EX4300 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 3: Licensed Features on EX4300 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • FBF • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 3: Licensed Features on EX4300 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List

Premium	Campus and access Layer 3	• Bidirectional Forwarding Detection (BFD)
		• CFM (IEEE 802.1ag)
		• IGMP version 1, IGMP version 2, and IGMP version 3
		• Multicast Source Discovery Protocol (MSDP)
		• OAM CFM
		• OSPF version 2 or OSPF version 3
		• FBF
		• Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
		• Real-time performance monitoring (RPM)
		• RIP IPv6 (RIPng)
		• Unicast reverse-path forwarding (unicast RPF)
		• Virtual router
		• VRRP
		• BGP and multiprotocol BGP (MBGP)
		• IS-IS
		• EVPN-VXLAN
		  • Supported only on EX4300-48MP switch.
		  • Requires the BGP for configuration.

Table 4 on page 12 describes the licensing support for soft-enforced features on EX4400 switches.

Table 4: Licensed Features on EX4400 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 4: Licensed Features on EX4400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • FBF • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 4: Licensed Features on EX4400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Premium	Campus and access Layer 3	• Bidirectional Forwarding Detection (BFD) • CFM (IEEE 802.1ag) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery Protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • FBF • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP • BGP and multiprotocol BGP (MBGP) • IS-IS • EVPN-VXLAN • Requires the BGP for configuration.

On EX4400 switch, the flow-based telemetry and MACsec features are hard-enforced. You'll need a license to use these features.

[See Flex Software License for EX Series Switches, Juniper Agile Licensing Guide, and Configuring Licenses in Junos OS.]

- **Junos Multi-Access User Plane support for 5G user plane function (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 21.2R1, Junos Multi-Access User Plane supports routers functioning as user plane functions (UPFs) in accordance with 3GPP Release 15 CUPS architecture. This provides high-throughput 5G fixed and mobile wireless service in non-standalone (NSA) mode. This includes support for the following:

  - N3, N4, N6, and N9 interface support
  - Roaming through the N9 interface
  - GPRS tunneling protocol, user plane (GTP-U) tunneling to the control plane
  - QoS Flow ID (QFI) support for 5G QoS flows

  [See Junos Multi-Access User Plane Overview.]

- **RSVP-TE supports preempting secondary LSPs that are signaled but not active (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, you can preempt secondary LSPs that are signaled but not active and configure the hold priority of the secondary standby label-switched path (LSP) for RSVP-Traffic Engineering (RSVP-TE). This helps to bring up non-standby secondary path LSPs with higher setup priority which are not able to come-up because of bandwidth crunch. To configure the non-active hold priority value for a secondary standby path, use the `non-active-hold-priority` statement at the [`edit protocols mpls label-switched-path <lsp-name> secondary <path-name>`] hierarchy level. You can set the priority from 0 through 7, where 0 is the highest priority and 7 is the lowest.

- **Unified policy support for firewall user authentication (SRX Series and vSRX)**—Starting in Junos OS Release 21.2R1, we support firewall user authentication in a security policy with dynamic applications (unified policy). You can configure pass-through or web authentication in the unified policy to restrict or permit users to access network resources.
  Firewall user authentication support in the unified policy provides an additional layer of protection in a network with dynamic traffic changes.

  [See Configure Firewall User Authentication with Unified Policies.]

- **Secure packet capture to cloud (EX4400)**—Starting in Junos OS Release 21.2R1, we support secure packet capture using Junos telemetry interface (JTI). You can use this feature to capture packets from a device and send them over a secure channel to an external collector (in the cloud) for monitoring and analysis. The maximum size of the packet you can capture is 128 bytes, including the packet header and the data within. Network professionals use real-time packet capture data to troubleshoot complex issues such as network and performance degradation and poor end-user experience.

  To use secure packet capture, include the **/junos/system/linecard/packet-capture** resource path using a Junos RPC call.

  For ingress packet capture, include the `packet-capture` option in the existing firewall filter configuration at the [`edit firewall family family-name filter filter-name term match-term then packet-capture`] hierarchy

level. Do this before you send packet capture sensor data to the collector and remove the `packet-capture` configuration after data is sent to the collector. After the capture is done, ingress packets with the filter match conditions are trapped to the CPU. The trapped packets then go to the collector over a secure channel in JTI-specified format in key-value pairs by means of Remote Procedure Call (gRPC) transport.

For egress packet capture on physical interfaces (ge-*, xe-*, mge-*, and et-*), include "packet-capture-telemetry," "egress," and "interface <interface-name>" at the `[edit forwarding-options]` hierarchy level. For example:

```
set forwarding-options packet-capture-telemetry egress interface ge-0/0/0

set forwarding-options packet-capture-telemetry egress interface ge-0/0/10
```

You can add multiple interfaces on the device for egress packet capture. When configured, host-bound egress packets are captured from the interface and sent to the collector. As with the ingress configuration, remove the configuration when packet capture is not required.

- **G.8275.1 Telecom profile and PTP over Ethernet encapsulation support (ACX2100 and ACX2200)**—Starting in Junos OS Release 21.2R1, ACX2100 and ACX2200 routers support Precision Time Protocol (PTP) over Ethernet encapsulation and G.8275.1 Telecom profile.

  The G.8275.1 Telecom profile supports the architecture defined in ITU-T G.8275 to enable the distribution of phase and time with full timing support. This profile requires all devices in the network to operate in combined or hybrid modes, which means that PTP and Synchronous Ethernet are enabled on all devices.

  PTP over Ethernet enables the effective implementation of packet-based technology that enables the operator to deliver synchronization services on packet-based mobile backhaul networks.

  [See G.8275.1 Telecom Profile and Precision Time Protocol Overview.]

- **Hardware-assisted inline BFD (QFX5120-32C and QFX5120-48Y)**—Starting in Junos OS Release 21.2R1, we support a hardware implementation of the inline BFD protocol in firmware form. The ASIC firmware handles most of the BFD protocol processing. The firmware uses existing paths to forward any BFD events that must be processed by protocol processes. The ASIC firmware processes the packets more quickly than the software, so hardware-assisted inline BFD sessions can have keepalive intervals of less than a second. These platforms support this feature for single-hop and multihop IPv4 and IPv6 BFD sessions.

  [See ppm and Bidirectional Forwarding Detection (BFD).]

- **Interoperability of MPC10E with MX-SPC3 for IPSec services steering (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.2R1, the MPC10E-15C-MRATE and MPC10E-10C-MRATE interoperates with the MX-SPC3 card to enable the packet forwarding path that steers packets to the MX- SPC3 card. The MPC10E line card can perform the ingress or the egress processing for

IPSec services packets through the `st0` and `vms` interfaces, nexthops, and the routes programmed in the line card.

[See MPC10E-15C-MRATE and MPC10E-10C-MRATE.]

- **Interoperability of MPC10E with MX-SPC3 to support TLB (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.2R1, the MPC10E-15C-MRATE and the MPC10E-10C-MRATE interoperates with the MX-SPC3 card to support traffic load balancing. Using the Traffic Load Balancer (TLB) application, you can distribute traffic among multiple servers in a server group and perform health checks to determine whether any servers should not receive traffic. TLB supports multiple VPN routing and forwarding instance (VRF) instances..

  [See Traffic Load Balancer Overview.]

- **MRU support (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.2R1, you can configure maximum receive unit (MRU) size to accept packet sizes which are bigger than the configured MTU size and configure different values for both MTU and MRU to prevent frequent fragmentation and reassembly of larger packets on the receiving side. You can configure MRU on the `xe`, `ge`, `et`, and `reth` interfaces.

  Use the CLI command `mru` under the `[edit interfaces` *`name`* `gigether-options]` hierarchy level to configure the MRU size in bytes.

  [See mru.]

- **Support for BGP MVPN (ACX710 routers)**—Starting in Junos OS Release 21.2R1, ACX710 routers support BGP multicast virtual private network (MVPN) (also known as next-generation (NG) MVPN). You can configure multipoint LDP provider tunnels as the data plane for intra-AS BGP MVPNs. ACX710 routers do not support extranet MVPN.

  [See Multiprotocol BGP MVPNs Overview.]

Junos OS Release Notes for ACX Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 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

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

What's New in 21.2R1

IN THIS SECTION

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

Dynamic Host Configuration Protocol

- **Support for persistent storage of DHCPv4 and DHCPv6 bindings over EVPN IRB (ACX5448, ACX5448-D, and ACX5448-M)**—Starting in Junos OS Release 21.2R1, ACX5448, ACX5448-D, and ACX5448-M routers that are configured to function as a DHCP relay agent can also be configured to preserve the DHCPv4 and DHCPv6 subscriber bindings across reboots. Existing bindings are written to a local file in **/var/preserve**. After reboot, the binding table is populated with the contents of the file, and the router identifies each subscriber that was on the deleted interface, and resumes normal packet processing for subscribers when the interface is restored. To preserve the subscriber binding information, enable the `perisistent-storage` statement at the `[edit system services dhcp-local-server]` hierarchy level.

  [See Preserving Subscriber Binding Information and DHCPv6 Relay Agent Overview.]

Ethernet Switching and Bridging

- **Support for L2PT over VPLS networks (ACX710, ACX5448, ACX5448-D, and ACX5448-M)**—Starting in Junos OS Release 21.2R1, we support Layer 2 protocol tunneling (L2PT) over virtual private LAN service (VPLS) networks. The device can use L2PT to transparently send packets across a VPLS network without interfering with protocol instances in the network. L2PT supports 802.1x, 802.3ah, CDP, E-LMI, MVRP, LACP, STP/RSTP/MSTP, LLDP, MMRP, and VTP Layer 2 control protocols.

  [See Layer 2 Protocol Tunneling and Configuring VPLS Encapsulation on CE-Facing Interfaces.]

- **Support for Ethernet Ring Protection (ACX5448, ACX5448-M, and ACX5448-D)**—Starting in Junos OS Release 21.2R1, you can use ERPS to reliably achieve carrier-class network requirements for Ethernet topologies forming a closed loop.

  [See Understanding Ethernet Ring Protection Switching Functionality .]

EVPN

- **Support for DHCP Option 82 over EVPN (ACX Series)**—Starting in Junos OS Release 21.2R1, Option 82 flags are inserted in the DHCP packets to enhance security when the packet is sent to the server.

The provider edge (PE) router that is part of the EVPN instance acts as the relay agent, and adds these flags to the DHCP packets.

DHCPv4 packet relay and DHCPv6 packet relay use this process. With the introduction of EVPN IRB, the relay agent uses the IRB interface with EVPN for forwarding the requests, and for replies to and from the client or the server instead of using the default routing option. If one PE router fails, an appropriate DHCPv6-PD state is made available for the remaining PE routers participating in the DHCP-PD process for the VLAN. This is done using automatic synchronization of DHCPv6-PD states between multiple PE routers that are connected to the same Ethernet segment identifier (ESI) through EVPN BGP messages.

[See Understanding DHCP Option 82

- **Support for DHCPv6-PD on EVPN IRB synchronization among multiple PE routers (ACX Series)**—You can use DHCPv6 prefix delegation (DHCPv6-PD) to automate the delegation of IPv6 prefixes to a requesting router on EVPN IRB. DHCPv6 prefix delegation is configured on EVPN IRB, and provides IPv6 prefixes to the requesting clients instead of a unique address. The DHCPv6-PD server acts as a provider edge (PE) router that provides the delegates through the relay (PE router) operating in the EVPN instance.

  If one PE router fails, an appropriate DHCPv6-PD state is made available for the remaining PE routers participating in the DHCP-PD process for the VLAN. This is done using automatic synchronization of DHCPv6-PD states between multiple PE routers that are connected to the same Ethernet segment identifier (ESI) through EVPN BGP messages.

Layer 2 VPN

- **Pseudowire redundancy support (ACX710)**—Starting in Junos OS Release 21.2R1, the ACX710 routers support pseudowire redundancy in Layer 2 circuits on multichassis link aggregation group (MC-LAG) routers.

  [See Understanding Pseudowire Redundancy Mobile Backhaul Scenarios.]

Multicast

- **Support for BGP MVPN (ACX710 routers)**—Starting in Junos OS Release 21.2R1, ACX710 routers support BGP multicast virtual private network (MVPN) (also known as next-generation (NG) MVPN). You can configure multipoint LDP provider tunnels as the data plane for intra-AS BGP MVPNs. ACX710 routers do not support extranet MVPN.

  [See Multiprotocol BGP MVPNs Overview.]

Network Management and Monitoring

- **Enhanced CFM support (ACX5448, ACX5448-M, and ACX5448-D)**—Starting in Junos OS Release 21.2R1, you can enable the performance monitoring responder functionality without enabling the transmission of continuity check messages (CCM). To enable the performance monitoring responder functionality without enabling CCM transmission, configure our new configuration statement `send-zero-interval-ccm` under the `[edit protocols protocols oam ethernet connectivity-fault-management]` hierarchy level. After you configure the statement, if the continuity-check is not enabled, CCMs are not transmitted, but are programmed to receive the CFM packets for that maintenance endpoint (MEP) level.

  [See IEEE 802.1ag OAM Connectivity Fault Management Overview and connectivity-fault-management (EX Series Switch Only).]

- **Support for port mirroring (ACX710)**—Starting in Junos OS Release 21.2R1, you can use analyzers to mirror copies of packets to a configured destination. You configure the analyzer at the `[edit forwarding-options analyzer]` hierarchy level.

  [See show forwarding-options analyzer.]

Routing Options

- **Enhancements to prefix-limit and accepted-prefix-limit configuration statements, and updates to show bgp neighbor command (ACX1000, EX9200, MX Series, PTX5000, and QFX10002)**— Starting from Junos OS Release 21.2R1, the `prefix-limit` and `accepted-prefix-limit` configuration statements include the following options:

  - `drop-excess <percentage>`—If you include the `drop-excess <percentage>` option and specify a percentage, the excess routes are dropped when the number of prefixes exceeds the specified percentage.

  - `hide-excess <percentage>`—If you include the `hide-excess <percentage>` option and specify a percentage, the excess routes are hidden when the number of prefixes exceeds the specified percentage.

  The `show bgp neighbor` command has been enhanced to display the following additional information:

  - Count of prefixes that are dropped or hidden based on network layer reachability information (NLRI) when the maximum allowed prefixes threshold is exceeded.

  - Alerts when a peer starts to drop or hide routes.

  - Configuration details of the `prefix-limit` and `accepted-prefix-limit` configuration statements.

  [See prefix-limit, accepted-prefix-limit, show bgp neighbor, and Multiprotocol BGP.]

Routing Protocols

- **Support for flexible algorithm in IS-IS for segment routing–traffic engineering (ACX Series)**—Starting in Junos OS Release 21.2R1, you can thin slice a network by defining flexible algorithms that compute paths using different parameters and link constraints based on your requirements. For example, you can define a flexible algorithm that computes a path to minimize IGP metric and define another flexible algorithm to compute a path based on traffic-engineering metric to divide the network into separate planes. This feature allows networks without a controller to configure traffic engineering and utilize segment routing capability of a device.

  To define a flexible algorithm, include the `flex-algorithm` statement at the `[edit routing-options]` hierarchy level.

  To configure participation in a flexible algorithm include the `flex-algorithm` statement at the `[edit protocols isis segment routing]` hierarchy level.

  [See Understanding IS-IS Flexible Algorithm for Segment Routing.]

- **Flexible algorithm inter-level leaking support for SRv6 and SR-MPLS in ISIS (ACX Series, MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support flexible algorithm inter-level leaking for SRv6 and SR-MPLS in IS-IS. Also, we partially support TE-App RFC 8919 in its basic form and extends 6PE support for flexible algorithm.

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Support for Layer 3 services over segment routing infrastructure (ACX710 routers)**—Starting in Junos OS Release 21.2R1, ACX710 routers support the following features:
  - IPv4 OSPF segment routing enabled through MPLS.
  - IS-IS segment routing enabled through MPLS.
  - Segment routing–traffic engineering (SR-TE).
  - Segment routing global block (SRGB) range label, which is used by Source Packet Routing in Networking (SPRING).
  - Anycast segment identifiers (SIDs) and prefix SIDs in SPRING.
  - Topology-independent loop-free alternate (TI-LFA) with segment routing, which enables fast rerouting.
  - MPLSlabel stack fast reroute (FRR) backup paths corresponding to the post-convergence path for a given failure.

[See Understanding Source Packet Routing in Networking (SPRING), Understanding Adjacency Segments, Anycast Segments, and Configurable SRGB in SPRING for IS-IS Protocol, and Understanding Topology-Independent Loop-Free Alternate with Segment Routing for IS-IS.]

System Management

- **G.8275.1 Telecom profile and PTP over Ethernet encapsulation support (ACX2100 and ACX2200)**—Starting in Junos OS Release 21.2R1, ACX2100 and ACX2200 routers support Precision Time Protocol (PTP) over Ethernet encapsulation and G.8275.1 Telecom profile.

  The G.8275.1 Telecom profile supports the architecture defined in ITU-T G.8275 to enable the distribution of phase and time with full timing support. This profile requires all devices in the network to operate in combined or hybrid modes, which means that PTP and Synchronous Ethernet are enabled on all devices.

  PTP over Ethernet enables the effective implementation of packet-based technology that enables the operator to deliver synchronization services on packet-based mobile backhaul networks.

  [See G.8275.1 Telecom Profile and Precision Time Protocol Overview.]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for ACX Series routers.

What's Changed in Release 21.2R1

IN THIS SECTION

Class of Service (CoS)

- Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

EVPN

- **Support for displaying SVLBNH information**—You can now view shared VXLAN load balancing next hop (SVLBNH) information when you display the VXLAN tunnel endpoint information for a specified ESI and routing instance by using `show ethernet-switching vxlan-tunnel-end-point esi` *`esi-identifier`* `esi-identifier instance` *`instance`* `svlbnh` command.

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python op scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the device passes command-line arguments to a Python op script, it prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device prefixes a single hyphen (-) to all argument names.

  [See Declaring and Using Command-Line Arguments in Op Scripts.]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

  When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

  [See request system scripts refresh-from and cert-file (Scripts).]

Network Management and Monitoring

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a

hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See Creating Action Scripts for YANG RPCs on Devices Running Junos OS and Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules.]

- **Changes to <commit> RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server's response for `<commit>` operations includes the following changes:

  - If a successful `<commit>` operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.
  - The NETCONF server response emits the `<source-daemon>` element as a child of the `<error-info>` element instead of the `<rpc-error>` element.
  - If you also configure the `flatten-commit-results` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server suppresses any `<commit-results>` XML subtree in the response and only emits an `<ok/>` or `<rpc-error>` element.

  [See Configuring RFC-Compliant NETCONF Sessions.]

- **Changes in contextEngineID for SNMPv3 INFORMS (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series**—Now the contextEngineID of SNMPv3 INFORMS is set to the local engine-id of Junos devices. In earlier releases, the contextEngineID of SNMPv3 INFORMS was set to remote engine-id.

  [See

  SNMP MIBs and Traps Supported by Junos OS..]

  See

Known Limitations

IN THIS SECTION

Learn about known limitations 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.

General Routing

- On the ACX710 routers, load-balancing does not working in the SMAC and DMAC incremental mode for VPLS/l2ckt. PR1477964
- On the ACX5448 routers, the two-way time error and CTE for 1 PPS do not meet the class A metrics.PR1535434
- On the ACX5448 routers, when you modify the MAC address, ping fails. PR1553472
- On the ACX7100-48L routers, session fails in the static multihop BFD IPv4/v6 session with routing-instance configuration and peer router. PR1569443

Open Issues

IN THIS SECTION

Learn about open issues 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.

General Routing

- On the ACX5448 routers, latency occurs for the host-generated ICMP traffic. PR1380145
- The circuit-cross-connect logs do not compress after rotation. PR1398511

- The rpd process might crash if the BGP route gets resolved over the same prefix protocol next-hop in the inet.3 table that has both the RSVP and LDP routes.PR1458595
- On the ACX710 routers with the console cable plugged in, system reboot might be interrupted. PR1513553
- On the ACX710 routers, alarm does not raise while booting the system with the recovery snapshot. PR1517221
- On the ACX5448 routers, ping stops working even though the ARP entry is present during continuous script executions. PR1533513
- The MC-LAG ICL interface needs to be configured as an aggregated Ethernet interface. PR1567790
- On the ACX5448 routers, the micro BFD session with VLAN-tagging gets stuck in the `Init` state. PR1574780
- The rpd process might get stuck at 100 percent due to the race condition. PR1582226
- The inline BFD stays down with the IS-IS or static clients. PR1561590
- On the ACX448 routers, the `packet buffer allocation failed` messages appears when you scale the CFM sessions with the SLA iterator. PR1574754
- On the ACX448 routers, high DMR out of sequence with iterator configuration occurs. PR1596050
- On the ACX710 routers, the `rpf-check-bytes` and `rpf-check-packets` counters do not get updated properly to the flat file as expected. PR1600513
- RLFA does not takes effect due to the service label appearing incorrectly. PR1577460
- On the ACX710 router, PTP might become nonresponsive and not function properly in certain condition. PR1587990
- On the ACX710 and ACX5400 routers, traffic might get forwarded through the member links remains in the `Down` state after you add new member links to the aggregated Ethernet interface. PR1589168
- On the ACX5448 router, the FPC might restart when you execute the `show firewall` command. PR1605288
- DHCP relay do not work in the routing-instance. PR1605854

Platform and Infrastructure

- Upon the receipt of specific sequences of genuine packets destined to the device, the kernel crashes and restarts. PR1557881

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R1

IN THIS SECTION

Class of Service (CoS)

- The explicit classifier or rewrite-rule might not work as expected for a logical interface when the configured wildcard. PR1556103
- FPC might crash might when you issue the `show class-of-service` command. PR1568661

General Routing

- The IPv6 BFD sessions with configuration below 100 ms flaps. PR1456237
- The aggregated Ethernet interface with LFM configured might not come up after reboot.PR1526283
- Packets might drop after configuring the PTP transparent clock.PR1530862
- On the ACX5448 routers, the BGPV6LU traffic drops when the node gets deployed in ingress. PR1538819
- In the Layer 3 VPN scenario, the CE device traffic drops on the ingress PE device while resolving using the default route in VRF. PR1551063
- Verification of multiple PD synchronizations with relay results in the deletion and addition of configurations. PR1554647
- The ACX5448 or ACX710 router as the TWAMP server delays the start session acknowledgment by 10 seconds. PR1556829
- On the ACX5448 routers, the unicast packets from the CE devices might be forwarded by the PE devices with an additional VLAN tag if IRB is used. PR1559084
- On the ACX5448 routers, single rate three color polices does not work. PR1559665
- On the ACX5048 routers, the fxpc process generates the core file on the analyzer configuration. PR1559690
- On the ACX2100 routers, laser-output-power occurs after disabling the interface and then rebooting. PR1560501
- On the ACX5448 routers, the following syslog message gets reported in every 30 seconds:

  ```
  ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_dyn_entry_counter_get : Entry is invalid.
  ```

  PR1562323
- On the ACX5048 routers, the MAC address entry with no traffic for the MAC age timer does not age out if an active traffic destined for the MAC is available. PR1565642
- Loopback0 firewall might not take effect along with error logs. PR1566417
- On the management interface of the ACX5448, ACX5448-D, and ACX5448-M routers, LLDP does not work. PR1566454
- On the ACX5448 and ACX710 routers, pushing more than 2 MPLS labels might not work. PR1566828

- The log file of the lcklsyncd process displays empty. PR1567687
- On the ACX500 routers, service MIC does not work.PR1569103
- On the ACX5048 routers, traffic-input-pps do not get incremented for VLAN tagged_flexible traffic. PR1569763
- On the ACX5448 routers, the untagged traffic gets incorrectly queued and marked. PR1570899
- On the ACX5448 routers, the RFC2544 reflector feature are not able to work on a higher port. PR1571975
- ARP traffic exceeding the polices limit does not get discarded. PR1573956
- Packets might get tagged with default VLAN-ID and dropped at the peer under the Layer 2 circuits local switching scenario. PR1574623
- The ACX Series router fails to process the RSVP path message. PR1576585
- Committing scheduler-map under class-of-service displays the following error message:

  ```
  LIBCOS_COS_TVP_FC_INFO_NOT_FOUND: Forwarding-class information not specified
  ```

  PR1579009
- On the ACX710 routers, configuration under auxiliary port causes continuous reboot. PR1580016
- An ACX router that runs DHCP Relay does not process packets received from the DHCP server if the packets arrive over MPLS with an explicit null label. PR1590225
- Traffic does not pass through circuit cross-connect interface with configured VLAN-ID range. PR1590969
- Packets might drop with all the commit events with the 1G speed configured interface. PR1524614
- On the ACX710 routers, unexpected results are observed while verifying the channelized interface check with the snmp mib get ifHighSpeed output. PR1583995
- On the ACX5448 routers, detection time shows the default value (6.000) instead of the configured value for a single hop BFD. PR1585382
- On the ACX710 routers, the size of the `jnpr-clock-recovery.log` log file is small and the archives rotate too quickly. PR1582350
- On the ACX710 routers, the l2ald process generates the core file at `l2ald_event_process_list_id`, `l2ald_event_proc_all_lists`, `l2ald_event_periodic ()` at **../../../../../../src/junos/usr.sbin/l2ald/l2ald_event.c:757**. PR1596908

- BUM traffic might be dropped in the VPLS instance under certain conditions. PR1531733
- On the ACX5448 router, the SFP-T interface might not come up if a straight cable is used. PR1547394
- When an RDI is received with CCM packet, sessions do not get deleted. PR1560182
- When the LACP daemon restarts, the LACP local partner system ID remains 0 in the `mc-ae` output. PR1560820
- Analyzer (Port Mirroring) might not work on ports above 20. PR1563774
- The DF (Designated Forwarder) might not forward traffic. PR1567752
- ACX routers reset the tunable optics to the default wavelength after an upgrade or reboot. PR1570192
- The l2circuit and CFM sessions might go down when you configure the `asynchronous-notification`. PR1572722
- On the ACX5448 and ACX710 routers, 802.1P rewrite might not work. PR1574601
- There might be a traffic drop between the customer edge and provider edge devices in case of the ARP resolution failure. PR1580782
- On the ACX710 and ACX5448 routers, DHCPv4 might not work. PR1589135
- On the ACX5448 and ACX710 routers, traffic drop occurs in the EVPN VPWS flexible cross connect. PR1598074

Routing Protocols

- The BGP session carrying VPNv4 prefix with IPv6 next-hop might be dropped. PR1580578

Documentation Updates

There are no errata and changes in Junos OS Release 21.2R1 for the ACX Series documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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 https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/software-installation-and-upgrade/software-installation-and-upgrade.html 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 19,4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.1.

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.

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

Junos OS Release Notes for cRPD

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 for the containerized routing protocol process (cRPD) container. 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

Learn about new features introduced in the Junos OS main and maintenance releases for cRPD.

What's New in 21.2R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for cRPD.

Platform and Infrastructure

- **Support for next-hop-based dynamic tunnels (cRPD)**—Starting in Junos OS Release 21.2R1, you can configure next-hop-based dynamic IP tunnels in the Linux kernel to provide a private and secure path on a public network. By default, MPLS-over-UDP tunnel is preferred over GRE tunnels. We support the following dynamic tunnels:

  - GRE
  - MPLS over UDP

  [See Next-Hop-Based Dynamic Tunnels, Configuring Next-Hop-Based MPLS-Over-UDP Dynamic Tunnels, and Dynamic Tunnels Overview.]

- **EVPN over VXLAN encapsulation (cRPD)**—Starting in Junos OS Release 21.2R1, we support the Layer 2 EVPN over VXLAN functionality.

  [See EVPN with VXLAN Data Plane Encapsulation and MAC-VRF L2 services.]

Routing Protocols

- **Basic MVPN support with BGP sharding (cRPD, JRR200, MX2020, PTX5000, and QFX10002)**—Starting in Junos OS 21.2R1, we support the basic multicast virtual private network (MVPN) functionalities with BGP sharding.

  NOTE: Sharding is not supported for the MVPN address family.

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for cRPD.

What's Changed in Release 21.2R1

EVPN

- **Option to set the MTU size for a VXLAN packet (cRPD)**– You can configure the maximum transmission unit (MTU) size for a VXLAN packets by using the `mtu` option at the [`edit routing-instances <instance-name> bridge-domains <bridge-domain-name> vxlan`] hierarchy. The supported range for the MTU size is from 100 to 65535 bytes.

Known Limitations

Learn about known limitations in this release for cRPD.

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

EVPN

- In cRPD, the CLI command to show system core files is not available. If the process crash or there are core files in cRPD, you need to log in to Docker explicitly and check (periodically) /var/crash/ for any process crash or core file generation. PR1546097
- Linux kernel does not allow port sharing between flow-based and non-flow based VXLAN tunnels. The cRPD port 4789 is currently used for evpn-type5 which is based on flow-based tunnel. Use l2-evpn-vxlan for non-flow based VXLAN tunnels using `set routing-instances <inst-name> bridge-domains <bd-name> vxlan destination-udp-port <port>` command. PR1579060

Open Issues

There are no open issues for CRPD in Junos OS Release 21.2R1.

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

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

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

Resolved Issues: 21.2R1

Routing Protocols

- The RPD process might crash while using BFD API to start the BFD sessions. PR1569040
- You can use CLI options to change default BGP listen port. PR1576728

Documentation Updates

This section lists the errata and changes in Junos OS Release 21.2R1 for the cRPD documentation.

Junos OS Release Notes for cSRX

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 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

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for cSRX.

What's New in 21.2R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for cSRX.

Platform and Infrastructure

- **cSRX support on AWS (cSRX)**—Starting in Junos OS Release 21.2R1, you can deploy cSRX Container Firewall in Amazon Web Services (AWS) Cloud using Amazon Elastic Kubernetes Services (Amazon EKS), which is a fully managed Kubernetes service.

  With cSRX, you can also set up automated service provisioning and orchestration, distributed and multitenant traffic security, centralized management with Juniper® Security Director (including dynamic policy and address update, remote log collections, security events monitoring), and scalable security services with small footprints.

  cSRX is available with 60 days free trial eval license (S-CSRX-A1 SKU). The eval license in cSRX expires after 60 days.

  You can purchase bring your own license (BYOL) from Juniper Networks or a Juniper Networks authorized reseller for using the software features on the cSRX. Use this license to customize your license, subscription, and support.

  [See cSRX Deployment Guide for AWS and Flex Software License for cSRX.]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for cSRX.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for cSRX.

Known Limitations

There are no known limitations for cSRX in Junos OS Release 21.2R1.

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

Open Issues

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

Platform and Infrsturcture

- cSRX use Ubuntu 18.04 release as base OS which contain Common Vulnerabilities and Exposures (CVEs). If you use any container image scanning tool again cSRX, they might see Medium, Informational or Low Vulnerabilities listed in the report. PR1577604

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 21.2R1

There are no resolved issues for cSRX in Junos OS Release 21.2R1.

Documentation Updates

There are no errata and changes in Junos OS Release 21.2R1 for the cSRX documentation.

Junos OS Release Notes for EX Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 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

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

What's New in 21.2R1

IN THIS SECTION

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

Hardware

IN THIS SECTION

- The following methods to protect the chassis from excessive current draw and temperature conditions are supported:
  - Configure Junos OS to automatically shut down the PSM, or raise an alarm and log the event when a field-effect transistor (FET) failure is detected in the power supply module (PSM) by using the specified command. [See thermal-health-check].
  - Configure upgrade of the PSM firmware that will take actionwhen there is an FET failure by using the specified command. [See request system firmware upgrade].
  - Configure Junos OS to raise an alarm and log events when a PSM with upgraded firmware version shuts down due to an FET failure, Junos OS on the attached device.
  - Configure a monitor to check how much power the chassis draws from the PSM using the specified command. If the system draws more power from the PSM than what it should consume, Junos OS raises an alarm or shuts down the system. [See watchdog (PSM)].
    [See Handling Thermal Health Events Using Thermal Health Check and PSM Watchdog].
- Support for CLD LED (EX4400 switches)—In Junos OS Release 21.2R1, we have enabled the Cloud LED on EX4400 switches. The feature is under development. To learn more about the LED, see EX4400 Switch Hardware Guide.

EX4400-24MP and EX4400-48MP Features

We've added the following features to the EX4400-24MP and EX4400-48MP switches in Junos OS Release 21.2R1.

- **Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches**

Feature	Description
Hardware	• **New EX4400 switch models**—In Junos OS Release 21.2R1, we introduce the following new models of the EX4400 switch: EX4400-24MP and EX4400-48MP. The EX4400-24MP model has 24 100-Mbps, 1-Gbps, 2.5-Gbps, 5-Gbps, or 10-Gbps RJ-45 ports on the front panel. The EX4400-48MP model has 36 100-Mbps, 1-Gbps, or 2.5-Gbps RJ-45 ports and 12 100-Mbps, 1-Gbps, 2.5-Gbps, 5-Gbps, or 10-Gbps RJ-45 ports on the front panel. These ports support IEEE 802.3bt Power over Ethernet (PoE-bt). The EX4400 switches provide connectivity for high-density environments and scalability for growing networks. Typically, EX4400 switches are used in large branch offices, campus wiring closets, and data centers. In data centers, you can position EX4400 switches as top-of-rack switches to provide connectivity for all devices in the rack. EX4400 switches are our first cloud-ready switches. You can deploy EX4400 switches in cloud networks and manage them by using Juniper Mist Wired Assurance. EX4400-24MP switches support 1050-W AC power supplies. EX4400-48MP switches support 1600-W AC power supplies. EX4400 switches support front-to-back or back-to-front airflow directions. EX4400 switches support channelization. [See Port Settings.] To install the EX4400 switch hardware and perform initial software configuration, routine maintenance, and troubleshooting, see EX4400 Switch Hardware Guide. See Feature Explorer for the complete list of features for any platform.
Authentication and access control	• • 802.1X authentication. [See 802.1X Authentication.] • Captive portal. [See Captive Portal Authentication.]

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description
Chassis	• PSU, fan, and temperature sensors are monitored as part of chassis FRU management and environment support for multi-rate switch. PSU management includes redundancy support and power budgeting. Fan management includes speed change based on ambient temperature. Temperature sensor monitoring provides periodic temperature sensor data for the smooth functioning of switch. When the temperature reported by various sensors crosses the specified threshold, then the fan speed increases or decreases. If the shutdown threshold is breached, then system shutdown is initiated. [See EX4400 Switch Hardware Guide.]
Class of service	• Support for Class of Service (CoS) configuration [See Class of Service User Guide (EX Series Switches Except EX4600 and EX9200 Switches).]

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description

EVPN	• Layer 3 VXLAN gateway in EVPN-VXLAN centrally routed bridging overlay or edge-routed bridging overlay networks is supported on standalone switches or a Virtual Chassis, and includes the following features:
	  • Default gateway using IRB interfaces to route traffic between VLANs. [See Using a Default Layer 3 Gateway to Route Traffic in an EVPN-VXLAN Overlay Network.]
	  • IPv6 data traffic routed through an EVPN-VXLAN overlay network with an IPv4 underlay. [See Routing IPv6 Data Traffic through an EVPN-VXLAN Network with an IPv4 Underlay.]
	  • EVPN pure Type 5 routes. [See Understanding EVPN Pure Type-5 Route.]
	  The Virtual Chassis doesn't support EVPN-VXLAN multihoming, but you can use the standalone switch as an EVPN-VXLAN provider edge device in multihoming use cases.
	• Enhancement in the number of supported VLANs and ports—We have increased the combined total number of VLANs and ports that can be supported on the EX4400 switches. The number of supported VLANs remains at 4093, but Junos OS no longer limits the total number of ports and VLANS that can be configured on EVPN-VXLAN. This enhancement applies only when you use the enterprise style of configuration while configuring the interfaces.
	  [See Understanding EVPN with VXLAN Data Plane Encapsulation.]
	• Support for the following Layer 2 VXLAN gateway features in an EVPN-VXLAN network:
	  • Active/active multihoming
	  • Proxy ARP use and ARP suppression, and Neighbor Discovery Protocol (NDP) use and NDP suppression on non-IRB interfaces
	  • Ingress node replication for broadcast, unknown unicast, and multicast (BUM) traffic forwarding
	  [See EVPN Feature Guide.]
	• Support for Layer 2 VXLAN gateway services in an EVPN-VXLAN network:
	  • 802.1X authentication, accounting, CWA authentication, and captive portal

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description
	• CoS • DHCPv4 and DHCPv6 snooping, dynamc ARP inspection (DAI), neighbor discovery inspection, IP source guard and IPv6 source guard, and router advertisement (RA) guard (no multihoming) • Firewall filters and policing • Storm control, port mirroring, and MAC filtering [See EVPN Feature Guide.]
High Availability	• High availability includes NSSU, GRES, NSB, and NSR. [See High Availability User Guide.]

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description
Interfaces	• Support for multi-rate ports on EX4400-24MP and EX4400-48MP switches that support higher scale and bandwidth. The EX4400-48MP switch contains a total of 48 ports, of which: • 36 ports (0-35) operate at 2.5-Gbps, 1-Gbps, and 100-Mbps speed. • 12 ports (36-47) operate at 10-Gbps, 5-Gbps, 2.5-Gbps, 1-Gbps, and 100-Mbps speed. The EX4400-24MP switch contains 24 ports that operate at 10-Gbps, 5-Gbps, 2.5-Gbps, 1-Gbps, and 100-Mbps speed. Both the switches support the following four-port extension modules. However, you can install only one module at a time in the chassis: • The native extension module EX4400-EM-4Y supports 25-Gbps speed. • The other extension module EX4400-EM-4S supports 10-Gbps speed. [See Channelizing Interfaces on EX4400 Switches.] • Support for optics Forward Error Correction (FEC)sensor diagnostics, interfaces node level failure and restoration, and logging of operational, administrative events, and errors. Support for laser output and laser receiver power management. [See Troubleshoot the EX4400 Components.] • Support for the IEEE 802.3bt standard for Power over Ethernet (PoE) and fast PoE—With fast PoE enabled, the switch saves PoE power settings across a reboot, and powers on the powered device (PD) at the initial stage of the boot (within a few seconds of switching on power) before the complete switch is booted. To configure fast PoE, use the command `set poe fast-poe`. [See Understanding PoE on EX Series Switches.]

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description
Junos Telemetry Interface	• JTI Packet Forwarding Engine and Routing Engine sensor support—Use the Junos telemetry interface (JTI) and remote procedure calls (gRPC) to stream statistics from the switches to an outside collector. The following Routing Engine statistics are supported: • LACP state export • Chassis environmentals export • Network discovery chassis and components • LLDP export and LLDP model • BGP peer information (RPD) • RPD task memory utilization export • Network discovery ARP table state • Network discovery NDP table state The following Packet Forwarding Engine statistics are supported: • Congestion and latency monitoring • Logical interface • Filter • Physical interface • NPU/LC memory • Network discovery NDP table state To provision a sensor to export data through gRPC, use the telemetry Subscribe RPC to specify telemetry parameters. [See Configuring a Junos Telemetry Interface Sensor (CLI Procedure), Configure a NETCONF Proxy Telemetry Sensor in Junos, and Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).]

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description

	• Secure packet capture to cloud—We support secure packet capture using Junos telemetry interface (JTI). You can use this feature to capture packets from a device and send them over a secure channel to an external collector (in the cloud) for monitoring and analysis. The maximum size of the packet you can capture is 128 bytes, including the packet header and the data within. Network professionals use real-time packet capture data to troubleshoot complex issues such as network and performance degradation and poor end-user experience.
	
	To use secure packet capture, include the **/junos/system/linecard/packet-capture** resource path using a Junos RPC call.
	
	For ingress packet capture, include the `packet-capture` option in the existing firewall filter configuration at the `[edit firewall family` *`family-name`* `filter` *`filter-name`* `term` *`match-term`* `then packet-capture]` hierarchy level. Do this before you send packet capture sensor data to the collector and remove the `packet-capture` configuration after data is sent to the collector. After the capture is done, ingress packets with the filter match conditions are trapped to the CPU. The trapped packets then go to the collector over a secure channel in JTI-specified format in key-value pairs by means of Remote Procedure Call (gRPC) transport.
	
	For egress packet capture on physical interfaces (ge-*, xe-*, mge-*, and et-*), include "packet-capture-telemetry," "egress," and "interface <interface-name>" at the `[edit forwarding-options]` hierarchy level. For example:
	
	`set forwarding-options packet-capture-telemetry egress interface ge-0/0/0`
	
	`set forwarding-options packet-capture-telemetry egress interface mge-0/0/10`
	
	You can add multiple interfaces on the device for egress packet capture. When configured, host-bound egress packets are captured from the interface and sent to the collector. As with the ingress configuration, remove the configuration when packet capture is not required.

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description

Layer 2 Features	• The following Layer 2 unicast features are supported on EX4400-24MP and EX4400-48MP switches:
	  • 802.1D
	  • 802.1w (RSTP)
	  • 802.1s (MST)
	  • BPDU protect
	  • Loop protect
	  • Root protect
	  • VSTP
	  • 802.1Q VLAN trunking
	  • 802.1p
	  • PVLAN
	  • Routed VLAN Interface (RVI)
	  • Layer 3 VLAN-tagged subinterfaces
	  • 4096 VLAN support
	  • Multiple VLAN Registration Protocol (802.1ak)
	  • MAC address filtering
	  • MAC address aging configuration
	  • Static MAC address assignment for interface
	  • Per VLAN MAC learning (limit)
	  • MAC learning disable
	  • Persistent MAC (sticky MAC)

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description
	• Link aggregation static and dynamic with LACP (fast and slow LACP) • LLDP • Uplink failure detection (UFD) • VXLAN Layer 2 gateway (EVPN) • Ethernet ring protection switching (ERPS) version 1 comprises the following Layer 2 features: • Revertive mode of operation of the Ethernet ring • Multiple ring instances on the same interfaces • Multiple ring instances on different interfaces • Interworking with Spanning Tree Protocol, Multiple Spanning Tree Protocol, and redundant trunk groups [See Ethernet Ring Protection Switching Overview.]

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description

Layer 3 Features	• The following Layer 3 unicast features are supported on EX4400-24MP and EX4400-48MP switches:
	  • BFD for RIP, OSPF, ISIS, BGP, PIM
	  • BGP 4-byte ASN support
	  • BGP Add Path (BGP-AP)
	  • Filter-based forwarding (FBF)
	  • IP-directed broadcast traffic forwarding
	  • IS-IS
	  • IPv4 BGP
	  • IPv4 MBGP
	  • IPv4 over GRE
	  • IPv6 BGP
	  • IPv6 CoS (BA, classification and rewrite, scheduling based on TC)
	  • IPv6 IS-IS
	  • IPv6 OSPFv3
	  • IPv6 ping
	  • IPv6 stateless auto-configuration
	  • IPv6 static routing
	  • IPv6 traceroute
	  • OSPFv2
	  • Path MTU discovery
	  • RIPv2

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description
	• Static routing • Unicast reverse path forwarding (unicast RPF) • Virtual router for ISIS, RIP, OSPF, and BGP • Virtual Router Redundancy Protocol (VRRP) • VRRPv3 • 32-way equal-cost multipath (ECMP) [See BGP User Guide, Routing Policies, Firewall Filters, and Traffic Policers User Guide, IS-IS User Guide, Security Services Administration Guide, and OSPF User Guide.]
Multicast	• IGMP snooping • IGMP: version 1, version 2, version 3 • Multicast Listener Discovery (MLD) snooping • PIM-SM, PIM-SSM, PIM-DM [See Multicast Protocols User Guide.]
Network management and monitoring	• Local and remote port mirroring, and remote port mirroring to an IP address (GRE encapsulation). [See Port Mirroring and Analyzers.] • sFlow network monitoring technology. [See sFlow Monitoring Technology.]
Routing policy and firewall filters	• Firewall filters and policers. [See Firewall Filters Overview.]

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description

Security	• Support for Media Access Control Security (MACsec) with 256-bit cipher suite. [See Understanding Media Access Control Security (MACsec).]
	• Support for the following port security features:
	  • DHCP snooping (IPv4 and IPv6)
	  • Dynamic ARP inspection (DAI)
	  • IPv6 neighbor discovery inspection
	  [See Security Services Administration Guide.]

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description

Software Installation and Upgrade	• Support for the phone-home client—The phone-home client (PHC) can securely provision an EX4400 Virtual Chassis without requiring user interaction. You only need to:
	  • Ensure that the Virtual Chassis members have the factory-default configuration.
	  • Interconnect the member switches using dedicated or default-configured Virtual Chassis ports.
	  • Connect the Virtual Chassis management port or any network port to the network.
	  • Power on the Virtual Chassis members.
	The PHC automatically starts up on the Virtual Chassis and connects to the phone-home server (PHS). The PHS responds with bootstrapping information, including the Virtual Chassis topology, software image, and configuration. The PHC upgrades each Virtual Chassis member with the new image and applies the configuration, and the Virtual Chassis is ready to go.
	[See Provision a Virtual Chassis Using the Phone-Home Client.]
	• **ZTP with IPv6 support**—You can use a DHCPv6 client and zero-touch provisioning (ZTP) to provision a device. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding the image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If one of the DHCPv4 bindings fails, the device continues to check for bindings until provisioning is successful. However, if there are no DHCPv4 bindings, the device checks for DHCPv6 bindings and follows the same process as for DHCPv4 until the device is provisioned successfully. Both DHCPv4 and DHCPv6 clients are included as part of the default configuration on the device.
	The DHCP server uses DHCPv6 options 59 and 17 and applicable suboptions to exchange ZTP-related information between itself and the DHCP client.
	[See Zero Touch Provisioning.]
	• **Support for DHCP option 43 suboption 8 to provide proxy server information in PHC**—During the bootstrapping process, the phone-home client (PHC) can access the redirect server or the phone-home server through a proxy server. The DHCP server uses DHCP option 43 suboption 8 or DHCP option 17 suboption 8 to deliver the details of both IPv4 and IPv6 proxy servers to the PHC. The DHCP daemon running on the target switch learns about the proxy servers in the initial DHCP cycle. The

Table 5: Features Supported by the EX4400-24MP and EX4400-48MP Switches *(Continued)*

Feature	Description
	daemon then populates either the **phc_vendor_specific_info.xml** files or the **phc_v6_vendor-specific_info.xml** files located at **/var/etc/** with vendor-specific information. [See Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client.]
Virtual Chassis	• Virtual Chassis support for all EX4400 switch models. You can connect up to 10 EX4400 switches in a Virtual Chassis, and manage them as a single device. [See EX4400 Switches in a Virtual Chassis.]

EVPN

- **Port-based VLAN bundle services for EVPN (EX9200)**—Starting in Junos OS Release 21.2R1, Junos OS supports port-based VLAN bundle services for EVPN on the EX9200 switch. The port-based VLAN bundle service maps the VLANs on a port to the same bundle service.

  [See VLAN Bundle Service for EVPN.]

- **EVPN Type 2 and Type 5 route coexistence (EX4650, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we support the coexistence of EVPN Type 2 and Type 5 routes in EVPN-VXLAN edge-routed bridging overlay fabrics. This feature enables more efficient traffic flow and better usage of Packet Forwarding Engine resources. The switch applies a preference algorithm when you enable Type 5 routes. For any destinations for which the switch has no Type 5 route, the switch uses Type 2 routes by default. Otherwise, the switch gives preference to:

  - Type 2 routes for local ESI interfaces (locally learned routes)
  - Type 5 routes for all other destinations within the data center or across data centers

  You can refine these preferences by configuring routing policies in the EVPN routing instance to control the Type 5 routes that the switch imports and exports.

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

- **Enhancement in the number of supported VLANs and ports (EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, and EX4400-48T switches)**—Starting with Junos OS Release 21.2R1, we have increased the combined total number of VLANs and ports that can be supported on the EX4400 switches. The number of supported VLANs remains at 4093, but Junos OS no longer limits

the total number of ports and VLANS that can be configured on EVPN-VXLAN. This enhancement applies only when you use the enterprise style of configuration when configuring the interfaces.

[See Understanding EVPN with VXLAN Data Plane Encapsulation.]

Forwarding Options

- **Remote port mirroring with VXLAN encapsulation (EX4650, QFX5120-32C, QFX5120-48T, and QFX5120-48Y switches)**—Starting in Junos OS Release 21.2R1, you can configure remote port mirroring in an EVPN-VXLAN environment. Remote port mirroring sends copies of packets to an output destination for remote monitoring. This feature supports VXLAN encapsulation of the mirrored packets so they can be sent to an output destination in a separate virtual network identifier (VNI) domain.

IPv6

- **Stateless address autoconfiguration (SLAAC) snooping over a Layer 2 EVPN-VXLAN gateway (EX4300-MP and EX4300-MP VC)**—Starting in Junos OS Release 21.2R1, you can enable SLAAC snooping on EX4300-MP switches in an Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) deployment. We support SLAAC snooping on CE-facing L2 interfaces. IPv6 clients using SLAAC for dynamic address assignment are validated against the SLAAC snooping binding table before being allowed access to the network.

  [See IPv6 Stateless Address Auto-configuration (SLAAC) Snooping.]

Junos Telemetry Interface

> **NOTE**: For Routing Engine telemetry sensors supported by this platform, see Telemetry Sensor Explorer. If any Platform Forwarding Engine sensors have been added for this release, they are listed below

- **End-of-message notification for Routing Engine sensors (EX2300, EX4300, EX4300-MP, EX9200, MX240, MX960, MX10016, MX2010, MX2020, PTX1000, PTX3000, PTX10001, QFX5100, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we've introduced an end-of-message (EoM) Boolean flag for all Junos telemetry interface (JTI) Routing Engine sensors. The flag notifies the collector that the current wrap has completed for a particular sensor path. A wrap is a complete key-value data dump for all the leaves under a sensor path.

  The EoM flag also enables the collector to detect when the end of wrap occurs without having to compare stream creation timestamp values that the collector receives from the packets. Comparing timestamp values is costly time-wise and delays data aggregation.

To use this feature with gRPC Network Management Interface (gNMI) transport or Remote Procedure Call (gRPC), retrieve the protobuf files from the relevant branch on the Juniper Networks download site:

- GnmiJuniperTelemetryHeaderExtension.proto (gNMI)
- agent.proto (for gRPC)

For example: https://github.com/Juniper/telemetry/blob/master/20.3/20.3R1/protos/GnmiJuniperTelemetryHeaderExtension.proto.

After you download and install the new protobuf files on a collector, the EoM field is present in the packets received.

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

- **Secure packet capture to cloud (EX4400)**—Starting in Junos OS Release 21.2R1, we support secure packet capture using Junos telemetry interface (JTI). You can use this feature to capture packets from a device and send them over a secure channel to an external collector (in the cloud) for monitoring and analysis. The maximum size of the packet you can capture is 128 bytes, including the packet header and the data within. Network professionals use real-time packet capture data to troubleshoot complex issues such as network and performance degradation and poor end-user experience.

  To use secure packet capture, include the **/junos/system/linecard/packet-capture** resource path using a Junos RPC call.

  For ingress packet capture, include the `packet-capture` option in the existing firewall filter configuration at the `[edit firewall family family-name filter filter-name term match-term then packet-capture]` hierarchy level. Do this before you send packet capture sensor data to the collector and remove the `packet-capture` configuration after data is sent to the collector. After the capture is done, ingress packets with the filter match conditions are trapped to the CPU. The trapped packets then go to the collector over a secure channel in JTI-specified format in key-value pairs by means of Remote Procedure Call (gRPC) transport.

  For egress packet capture on physical interfaces (ge-*, xe-*, mge-*, and et-*), include "packet-capture-telemetry," "egress," and "interface <interface-name>" at the `[edit forwarding-options]` hierarchy level. For example:

  ```
  set forwarding-options packet-capture-telemetry egress interface ge-0/0/0

  set forwarding-options packet-capture-telemetry egress interface ge-0/0/10
  ```

  You can add multiple interfaces on the device for egress packet capture. When configured, host-bound egress packets are captured from the interface and sent to the collector. As with the ingress configuration, remove the configuration when packet capture is not required.

Licensing

- **Juniper Agile Licensing (EX2300, EX3400, EX4300, and EX4400)**—Starting in Junos OS Release 21.2R1, the listed EX Series switches support Juniper Agile Licensing.

  Juniper Agile Licensing provides simplified and centralized license administration and deployment. You can use Juniper Agile Licensing to install and manage licenses for hardware and software features.

  Juniper Agile Licensing supports soft enforcement and hard enforcement of hardware and software feature licenses.

  - With soft enforcement, if you configure a feature without a license, Junos OS displays a warning when you commit the configuration. However, the feature remains operational. In addition, Junos OS generates periodic alarms indicating that you need the license to use the feature. You can see the list of alarms at System Log Explorer.

  - With hard enforcement, if you configure a feature without a license, Junos OS displays a warning when you commit the configuration. The feature is not operational until the license is installed. In addition, Junos OS generates periodic syslog messages indicating that you need the license to use the feature. You can see the list of syslog messages at System Log Explorer.

  Table 6 on page 60 describes the licensing support for soft-enforced features on EX2300 switches.

Table 6: Licensed Features on EX2300 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operation, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis*

Table 6: Licensed Features on EX2300 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRP version 3 • Multicast Source Discovery protocol (MSDP) • OAM and Maintenance CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • VRRP

Virtual Chassis*—We've included Virtual Chassis license in the Standard license model on EX2300-C 12-port switches. However, we don't include the Virtual Chassis license on EX2300 24-port and 48-port switch models. You need to purchase the license separately.

Table 7 on page 62 describes the licensing support for soft-enforced features on EX3400 switches.

Table 7: Licensed Features on EX3400 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 7: Licensed Features on EX3400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRP version 3, and virtual router support for unicast • Filter-based forwarding (FBF) • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 7: Licensed Features on EX3400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Premium	Campus and access Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRPv3, virtual router support for unicast, and FBF • Multicast Source Discovery Protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP • BGP and multiprotocol BGP (MBGP) • IS-IS

Table 8 on page 65 describes the licensing support for soft-enforced features on EX4300 switches.

Table 8: Licensed Features on EX4300 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 8: Licensed Features on EX4300 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • FBF • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 8: Licensed Features on EX4300 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List

Premium	Campus and access Layer 3	• Bidirectional Forwarding Detection (BFD)
		• CFM (IEEE 802.1ag)
		• IGMP version 1, IGMP version 2, and IGMP version 3
		• Multicast Source Discovery Protocol (MSDP)
		• OAM CFM
		• OSPF version 2 or OSPF version 3
		• FBF
		• Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
		• Real-time performance monitoring (RPM)
		• RIP IPv6 (RIPng)
		• Unicast reverse-path forwarding (unicast RPF)
		• Virtual router
		• VRRP
		• BGP and multiprotocol BGP (MBGP)
		• IS-IS
		• EVPN-VXLAN
		  • Supported only on EX4300-48MP switch.
		  • Requires the BGP for configuration.

Table 9 on page 68 describes the licensing support for soft-enforced features on EX4400 switches.

Table 9: Licensed Features on EX4400 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • Q-in-Q • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 9: Licensed Features on EX4400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • FBF • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 9: Licensed Features on EX4400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Premium	Campus and access Layer 3	• Bidirectional Forwarding Detection (BFD) • CFM (IEEE 802.1ag) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery Protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • FBF • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP • BGP and multiprotocol BGP (MBGP) • IS-IS • EVPN-VXLAN • Requires the BGP for configuration.

On EX4400 switch, the flow-based telemetry and MACsec features are hard-enforced. You'll need a license to use these features.

[See Flex Software License for EX Series Switches, Juniper Agile Licensing Guide, and Configuring Licenses in Junos OS.]

Network Management and Monitoring

- **Support for syslog over TLS (EX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, you can transport syslog (control plane) over Transport Layer Security (TLS) protocol. Encapsulating syslog over TLS allows you to:

  - Validate the remote destination (syslog server) before transmitting any sensitive syslog information. (Authentication)
  - Encrypt the syslog during the transport. (Encryption)
  - Verify that the data has not been modified or tampered with (Integrity)

  Before you enable this feature, ensure you:

  - Configure public key infrastructure (PKI) in Junos
  - Configure and load the digital certificates
  - Configure the remote destination (syslog server) that supports syslog over TLS

  To enable transport of syslog (control plane) over TLS, use the `tls` statement at the [`edit system syslog host host-name transport`] hierarchy level.

Routing Options

- **Enhancements to prefix-limit and accepted-prefix-limit configuration statements, and updates to show bgp neighbor command (ACX1000, EX9200, MX Series, PTX5000, and QFX10002)**— Starting from Junos OS Release 21.2R1, the `prefix-limit` and `accepted-prefix-limit` configuration statements include the following options:

  - `drop-excess <percentage>`—If you include the `drop-excess <percentage>` option and specify a percentage, the excess routes are dropped when the number of prefixes exceeds the specified percentage.
  - `hide-excess <percentage>`—If you include the `hide-excess <percentage>` option and specify a percentage, the excess routes are hidden when the number of prefixes exceeds the specified percentage.

  The `show bgp neighbor` command has been enhanced to display the following additional information:

  - Count of prefixes that are dropped or hidden based on network layer reachability information (NLRI) when the maximum allowed prefixes threshold is exceeded.
  - Alerts when a peer starts to drop or hide routes.
  - Configuration details of the `prefix-limit` and `accepted-prefix-limit` configuration statements.

  [See prefix-limit, accepted-prefix-limit, show bgp neighbor, and Multiprotocol BGP.]

Software Installation and Upgrade

- **Support for DHCP option 43 suboption 8 to provide proxy server information in PHC (EX2300-C, EX2300-MP, EX4300, EX4300-MP, EX4300-VC, EX4600-VC, EX4650, and EX4650-48Y-VC)**—Starting in Junos OS Release 21.2R1, during the bootstrapping process, the phone-home client (PHC) can access the redirect server or the phone-home server through a proxy server. The DHCP server uses DHCP option 43 suboption 8 or DHCP option 17 suboption 8 to deliver the details of both IPv4 and IPv6 proxy servers to the PHC. The DHCP daemon running on the target switch learns about the proxy servers in the initial DHCP cycle. The daemon then populates either the **phc_vendor_specific_info.xml** files or the**phc_v6_vendor-specific_info.xml** files located at **/var/etc/** with vendor-specific information.

  [See Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client.]

- **ZTP with IPv6 support (EX2300-C, EX2300-MP, EX4300, EX4300-MP, EX4300-VC, EX4600-VC, EX4650, and EX4650-48Y-VC)**—Starting in Junos OS Release 21.2R1, you can use a DHCPv6 client and zero-touch provisioning (ZTP) to provision a device. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding the image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If one of the DHCPv4 bindings fails, the device continues to check for bindings until provisioning is successful. However, if there are no DHCPv4 bindings, the device checks for DHCPv6 bindings and follows the same process as for DHCPv4 until the device is provisioned successfully. Both DHCPv4 and DHCPv6 clients are included as part of the default configuration on the device.

  The DHCP server uses DHCPv6 options 59 and 17 and applicable suboptions to exchange ZTP-related information between itself and the DHCP client.

  [See Zero Touch Provisioning.]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for EX Series switches.

What's Changed in Release 21.2R1

IN THIS SECTION

Class of Service (CoS)

- Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

EVPN

- **IGMP snooping options has changed hierarchy level**–Junos OS has moved the following options from the **edit protocols igmp-snooping** hierarchy to **edit protocols igmp-snooping vlan <vlan-name/vlan-all>** hierarchy and **edit routing-instances evpn protocols igmp-snooping** hierarchy to **edit routing-instances evpn protocols igmp-snooping vlan <vlan-name/vlan-all>** hierarchy:
  - query-interval
  - query-last-member-interval
  - query-response-interval
  - robust-count
  - evpn-ssm-reports-only
  - immediate-leave
- **Support for displaying SVLBNH information**—You can now view shared VXLAN load balancing next hop (SVLBNH) information when you display the VXLAN tunnel endpoint information for a specified ESI and routing instance by using `show ethernet-switching vxlan-tunnel-end-point esi` *`esi-identifier`* `esi-identifier instance` *`instance`* `svlbnh` command.

General Routing

- **Configure internal IPsec authentication algorithm (EX Series)**—You can configure the algorithm `hmac-sha-256-128` at the **`edit security ipsec internal security-association manual direction bidirectional authentication algorithm`** hierarchy level for internal IP security (IPsec) authentication. In earlier releases, you could configure the algorithm `hmac-sha-256-128` for MX Series devices only.

Interfaces and Chassis

- **Blocking duplicate IP detection in the same routing instance (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, and SRX Series)**—Junos OS will no longer accept duplicate IPs between different logical interfaces in the same routing instance. Refer to the table mentioned in the topic inet (interfaces). When you try to configure same IP on two logical interfaces inside same routing instance, the commit will be blocked with the error displayed as shown below: `edit user@host# set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.2/24`, `edit user@host# commit commit complete`, `edit user@host# set interfaces ge-0/0/2 unit 0 family inet address 2.2.2.2/24 , edit user@host# commit`, and `edit interfaces ge-0/0/2 unit 0 family inet 'address 2.2.2.2/24' identical local address found on rt_inst default, intfs ge-0/0/2.0 and ge-0/0/1.0, family inet. error: configuration check-out failed`

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python op scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the device passes command-line arguments to a Python op script, it prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device prefixes a single hyphen (-) to all argument names.

  [See Declaring and Using Command-Line Arguments in Op Scripts.]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

  When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See request system scripts refresh-from and cert-file (Scripts).]

Network Management and Monitoring

- **Chef and Puppet support removed (EX Series except EX4400, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, Junos OS products that were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS. FreeBSD 12.x based Junos OS does not support installing existing Chef or Puppet packages.

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

  [See Creating Action Scripts for YANG RPCs on Devices Running Junos OS and Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules.]

- **Changes to `<commit>` RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server's response for `<commit>` operations includes the following changes:

  - If a successful `<commit>` operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.

  - The NETCONF server response emits the `<source-daemon>` element as a child of the `<error-info>` element instead of the `<rpc-error>` element.

  - If you also configure the `flatten-commit-results` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server suppresses any `<commit-results>` XML subtree in the response and only emits an `<ok/>` or `<rpc-error>` element.

  [See Configuring RFC-Compliant NETCONF Sessions.]

- **Changes in contextEngineID for SNMPv3 INFORMS (PTX Series, QFX Series, ACX Series, EX Series, MX Series, and SRX Series**--Now the contextEngineID of SNMPv3 INFORMS is set to the local engine-id of Junos devices. In earlier releases, the contextEngineID of SNMPv3 INFORMS was set to remote engine-id.

  [See SNMP MIBs and Traps Supported by Junos OS.]

Known Limitations

Learn about known limitations 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.

General Routing

- The Junos OS might hang trying to acquire the SMP IPI lock while rebooting when it is running as a VM on the Linux and the QEMU hypervisor. As a workaround, you can power cycle the device. PR1385970
- On a Virtual Chassis, the CLI command to add license is not available on the backup member. Virtual Chassis master installs the Licenses in all the VC members.PR1545075
- Packets are mirrored through analyzer with ingress and egress interfaces across different virtual chassis members might have a different vlan-id from that of vlan-id of the exiting egress interface. This limitation is from underling hardware. PR1552905
- "Resource deadlock avoided" messages are observed when `request system software add` statement is issued on EX4400 line of switches. No functionality impact is seen. PR1557468
- On the EX4400 Virtual Chassis, software upgrade using the Non Stop Software Upgrade functionality might fail for 21.2R1 images. The Backup member will be upgraded to target image first and the backup member might not become ready for GRES within required time when upgraded to target image. The Non Stop Software Upgrade process aborts with error. You must manually restore the backup member to previous software version. PR1599506

Open Issues

IN THIS SECTION

Platform and Infrastructure | 81

Learn about open issues 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.

EVPN

- On all Junos OS platforms with EVPN-VxLAN scenario, the number of MAC-IP binding counters might reach the limit when MAC-IP is moved between interfaces. Since MAC-IP counters are not decremented when entry is deleted due to this defect, repeated moves will result in a limit (default value is 1024) that will be reached even though there are fewer entries. Meanwhile, traffic loss could be seen. PR1591264
- On all Junos OS platforms traffic loss might be seen if an aggregated Ethernet bundle interface with ESI is disabled on master Routing Engine followed by a Routing Engine switchover. PR1597300

General Routing

- On the EX9214 device, if the MACsec-enabled link flap after reboot, the following error messgae appears:

  ```
  errorlib_set_error_log(): err_id(-1718026239)
  ```

  PR1448368
- The `show pfe filter hw filter-name` does not retrieve the Packet Forwarding Engine program. PR1495712
- On the EX4300-48MP line of switches, the reboot time, FPC and interface uptimes are degraded by 20 percent when compared to Junos OS Releases 19.1R3, 19.2R2, and 19.4R2. PR1514364
- On EX Series line of switches with Virtual Chassis (VC) scenario, Power over Ethernet (POE) might not be detected and hence might fail to work on VC members. This happens when there is a CPU

spike on master (for example, 70 percent or above) and if a VC member gets rebooted or a new member joins VC. It is a rare timing issue and hard to reproduce. PR1539933

- The rpd process might crash and generate a core file when the telemetry data for a streamed node is deleted during a network churn. The same node is being walked or rendered for the sensor. In this corner case the rendering and deletion of a particular node occurs at the same instance. This issue can occur only in case of an unstable network. PR1552816
- On the EX4400 line of switches, the following error messages appears when the software is upgraded.

```
Resource deadlock avoided
```

PR1557468

- On EX Series and EX Series VC platforms, post Routing Engine switchover, MAC address is configured to IRB interface (for example, set interface irb.500 mac 00:11:22:33:44:55) on new master Routing Engine, then the new master Routing Engine might crash or go into DB mode. PR1565213
- Traffic drops during ISSU due to flapping of the LAG interface flap. PR1569578<xref
- On a EX4400 VC, the SNMP MIB object jnRedundencySwitchOverCount will display the number of times the mastership of the Routing Engine that is changed between master and backup roles. This counter will not be reset to 0 when entire VC is rebooted. The count displayed under "jnRedundencySwitchOverCount" will be the cumulative value of the switchover events. PR1570359
- On the EX4600-40F line of switches, EVPN_VXLAN get unexpected multicast traffic streams after enabling EVPN. PR1570689
- On all Junos OS platforms, traffic loss might be observed because of the rare timing issue when performing frequent Interface Bridge Domain (IFBD) configuration modifications. This behavior is seen when the Packet Forwarding Engine receives out-of-order IFBD(s) from Routing Engine and might lead to the fxpc process crash and traffic drop. PR1572305
- The dcpfe process generates a core file with a MAC based VLAN scale configuration after the interface flaps. PR1578859
- On the EX Series platforms, a few 40G ports might not be channelized successfully and might stay down after upgrading host OS along with Junos OS using ZTP or doing manually through CLI. PR1582105
- USB boots on upgrading to Junos OS Release 21.2R1 and gets stuck in windriver mode. PR1582592
- On a EX4400 VC with 4 members, log messages related to fan settings will be saved in chassis traceoptions file at every 5 second interval. Though there is no implication of these messages, the

chassis trace log files will get overwritten with these logs at a faster rate. Log messages which will be written into the chassis traceoptions file. Fan id: 0, setting=3 val=0 Fan id: 1, setting=3 val=0 PR1594446

- On EX4400 platforms, if image upgrade is attempted using non-stop software upgrade, an error message "error: syntax error: request-package-validate" will be reported as the CLI output. The error does not have any impact on the non-stop software upgrade process. PR1596955
- On all Junos OS platforms with EVPN-VxLAN environment, when MAC/IP is moved from one Ethernet segment identifier (ESI) to another ESI from the same peer, the MAC/IP withdraw route might not be sent to the remote Virtual Tunnel End Point (VTEP), only MAC withdraw route is sent to the remote VTEP. PR1597391
- EX4400 platforms have a Cloud LED on the front panel to indicate 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 displays green in situations where device has lost connectivity to cloud. This is because, MIST is using outbound SSH for management. This behavior is not applicable to any other management entity that uses outbound https and LED that displays appropriate states to indicate the loss on connection to cloud. PR1598948
- On the EX4400 Virtual Chassis operating with scaled configurations and traffic, the line card console might fail to redirect to the current virtual chassis master member. User will be logged into line card and not all cli functionality will be available on the line card. Use the `request session member <virtual_chassis_member_id>` command from line card cli prompt to login to virtual chassis member cli. PR1599625
- On EX2300, after Virtual Chassis split and restore, L2/L3 unicast/multicast partial traffic loss might be observed. PR1600309
- There is a remote possibility that during many reboots, the Junos VM goes into a state where NMI is needed to continue the reboot. There is no workaround for this and a subsequent reboot does not seem to hit this issue. PR1601867
- On a EX4400 VC, when inband management IRB interface is not assigned with IP address or there is no DNS configured on the device, the cloud LED will display the pattern for "NO_CLOUD_RESPONSE" state of instead of NO-IP-Addr" or NO-DNS". This issue will not be observed on a standalone EX4400. PR1602664
- On EX4400 dot1x authentication might not work on EVPN/VXLAN enabled endpoints. The issue is due to EAPOL packets received on VxLAN ports are not processed in hostpath. PR1603015
- When a EX4400 Virtual Chassis is operating under scaled configurations and stressed traffic, a fxpc core file might be observed during any mastership switchover event. PR1603602
- A EX4400 POE model supplies power over ethernet to connected powered devices. Whenever POE firmware needs to be upgraded, the following CLI should be used for upgrading the POE firmware.

`request system firmware upgrade poe fpc-slot fpc-slot poe-bt-firmware`. The `poe-bt-firmware` statement is mandatory. If upgrade is triggered using "request system firmware upgrade poe fpc-slot fpc-slot", then the output of firmware upgrade process using "show poe controller" will show that the firmware upgrade process is stuck in SW_DOWNLOAD phase forever and the power may not be supplied to the PD's during this state. PR1606276

Infrastructure

- A double free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. See https://kb.juniper.net/JSA11162PR1497768
- When receives a unicast EAPOL (0x888e) with vlan588 tag at ae1 in this example, the packet is forwarded to ae0 without changing the vlanID to 3054. set vlans vlan588 vlan-id 588 set vlans vlan588 interface ae1.0 set vlans vlan588 interface ae0.0 mapping 3054 swap PR1580129
- On a EX4400 device, the cli command "show system processes detail" will not display CPU details under the CPU column. This issue is fixed from software version 21.3R1 onwards. PR1588150
- On a EX4400 device, a cloud LED on the device indicates the phone home client states and device connectivity state with the cloud. When the grpc application is configured with non-root user, then the cloud LED will not display any pattern related to day1 states. The LED pattern will still be displaying the previous day0 state as applicable. PR1589321
- EX2300, EX2300-MP, and EX3400 do not take kernel core file to internal storage on panic with Junos 21.2R1. PR1600442

Interfaces and Chassis

- On Junos platforms with VRRP failover-delay configured, changing VRRP mastership might cause peer device to re-learn VIP ARP entry on old master interface due to timing issue. PR1578126

Junos XML API and Scripting

- On a EX4400 device, any files scheduled for download using the cli command `request system download` might fail due to error. The files can be downloaded using normal ftp/scp commands on the device. PR1604622

Platform and Infrastructure

- When the dhcp relay mode is configured as no-snoop, the offer gets dropped due to incorrect ASIC programing. PR1530160
- On EX9200 line of switches, FPC gets restarted and thereby disrupting traffic when there is an out-of-order filter state. This issue might be seen only in back-to-back GRES in more than 40 to 50 iterations. PR1579182
- On EX4300 POE switches, the pfex process CPU utilization becomes high after 6-8 weeks. There is no functional impact. PR1453107
- A buffer overflow vulnerability in the TCP/IP stack of Juniper Networks Junos OS allows an attacker to send specific sequences of packets to the device thereby causing a Denial of Service (DoS). Refer to https://kb.juniper.net/JSA11200 for more information. PR1557881
- On EX9200 platforms, FPC gets restarted and thereby disrupting traffic when there is an out-of-order filter state and its terms, this issue might be seen only in back-to-back GRES in more than 40 to 50 iterations. PR1579182
- On EX4300 platforms, when a firewall filter for broadcast traffic with discard action policer is applied to the loopback interface, all broadcast packets (including Layer 2 forwarding packets, such as DHCP discover packets) that match this filter rule might be dropped. PR1597548
- On EX4300 platforms with both enterprise style and service provider style configurations, an interface with enterprise style logical interfaces and `flexible-vlan-tagging` configured, VLAN tagged traffic might be dropped due to incorrect programming in the system. PR1598251
- 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
- When Slaac-Snooping is enabled in VLAN, it is observed that sometimes due to the socket connection failure in Slaac-Snoopd daemon the DAD packet transmission from switch towards the client fails over the vtep interface. The DAD packet is intended to provoke NA response from CLIENT in order to renew the lease timer of the Global IPv6 entry in the switch and due to the DAD tx failure the Global IPv6 entry learnt over vtep interface is removed from slaac-snooping binding table on the switch. The Global IPv6 entry will get relearnt upon getting another DAD or NS packet from CLIENT in future. PR1603269

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R1

IN THIS SECTION

Class of Service (CoS)

- The buffer allocation for VCP ports might not get released in Packet Forwarding Engine after physically moving the port location. PR1581187

Forwarding and Sampling

- Configuration archive `transfer-on-commit` fails when running Junos OS Release 18.2R3-S6.5. PR1563641

General Routing

- When you rename a Virtual Chassis, the SNMP POE MIB walk produce either no results or sometimes show result from the primary Virtual Chassis. PR1503985
- The OSPF neighborship gets stuck in the Start state after configuring the EVPN-VXLAN. PR1519244
- Packet drops with all commit events with 1G speed configured interface. PR1524614
- High EVENTD CPU utilization upon receiving LLMNR and MDNS traffic on EX2300. PR1544549
- The device might be out of service after configuring the em1 or em2 interface. PR1544864
- Two Routing Engines might lose communication if they have different Junos OS versions on MX10003 and EX Series switches. PR1550594
- "Cattle-Prod Daemon received unknown trigger (type Semaphore, id 1)" error messages are seen on the vty when the CLI commands to fetch host route scale are issued. PR1554140
- OIR of CBs might result in major errors and the Packet Forwarding Engine disable action halted traffic forwarding on the FPCs. PR1554145
- The link on the Linux based LC is not brought down immediately after the FPC process(ukern/indus.elf) crashes or the process is killed PR1554430
- Traffic might be dropped when a firewall filter rule uses the then VLAN action. PR1556198
- FPC with power related faults might get on-lined again once Fabric Healing has off-lined the FPC. PR1556558
- On the EX4300 device, script fails while committing the IPSec authentication configuration as the algorithm statement is missing. PR1557216
- The MAC addresses learned in a Virtual Chassis might fail due to aging out in the MAC scaling environment. PR1558128
- The rpd process generates a core file after the Routing Engine switchover. PR1558814
- 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 tunable optics SFP+-10G-T-DWDM-ZR does not work on EX Series devices. PR1561181

- When `dot1x server-fail-voip vlan-name` is configured, ensure that both `server-fail-voip vlan-name` and `voip vlan` are configured using vlan-name and not by using vlan-id. PR1561323
- When you open the configuration database, "Could not open configuration database during usb upgrading" error is seen. PR1561741
- EX3400VC - SMARTD pollutes syslog every 5 seconds after the upgrade or when the system reboots. PR1562396
- If a license key has features that are not applicable on the platform (unknown features), the license key is rejected. If the license key has one or more platform applicable features (known features) along with unknwon features, license key addition is successful with LICENSE_INVALID_FEATURE_ID syslog warning message for the unknown features. PR1562700
- On EX3400-VC line of switches, the DAEMON-7-PVIDB throws syslog messages for every 12 to 14 minutes after you upgrade to Junos OS Release 19.1R3-S3. PR1563192
- Client authentication is failing after performing GRES. PR1563431
- The JWeb upgrade might fail on EX2300 and EX3400 line of switches. PR1563906
- The DHCP client might not obtain IP address when dhcp-security is configured PR1564941
- The Packet Forwarding Engine telemetry data might not be streamed out in EX Series Virtual Chassis. PR1566528
- On EX4600 platform, internal comment 'Placeholder for QFX Series platform configuration' might be seen on performing `show config` CLI command. PR1567037
- RPD core file is generated when the device reboots and the daemon restarts. No service impact is observed when the deamon restarts using the routing protocol. PR1567043
- EX2300 shows high FPC CPU usage. PR1567438
- The Designated Forwarder (DF) might not forward traffic. PR1567752
- The 40G DAC connection between EX9253 and the peers might not come up. PR1569230
- Packet loss might be observed when sample based action is used in firewall filter. PR1571399
- Port-mirroring might not work when the analyzer output is a trunk interface. PR1575129
- Protocol convergence between end nodes might fail when L2PT is enabled on transit switch. PR1576715
- The device implemented with different service image version might become VC member as unexpected. PR1576774
- MVR configuration cannot be configured on EX2300-C switches. PR1577905

- The fxpc process might crash on EX Series platforms. PR1578421
- Random/silent reboot might be seen on EX2300-24MP/EX2300-48MP platforms. PR1579576
- The voice VLAN might not get assigned to the access interface. PR1582115
- The l2ald crash if a specific naming format is applied between a vlan-range and a single vlan. PR1583092
- When EX2300-MP in standalone mode is used as a DHCP server, initial set of packets received in the server might get dropped. PR1583983
- After performing NSSU, "timeout waiting for response from fpc0" error message is seen while checking version details. PR1584457
- DSCP rewriting might fail to work on EX2300 switches. PR1586341
- The reserved multicast traffic (224.0.0.0/24) might be dropped if IGMP-snooping with pdu-block-on-edge is configured. PR1586970
- The SNMP trap for MAC notifications might not be generated when an interface is added explicitly under switch-options. PR1587610
- The rpd crash might be observed on the router running a scaled setup. PR1588439
- Packet loss could be observed on dynamically assigning VoIP VLAN. PR1589678
- Inconsistent statistics value is seen on performing `slaac-snooping`. PR1590926
- The LLDP packet might loose on the EX-4300MP platform if LLDP is configured on the management interface. PR1591387
- The `show pfe filter hw` command might generate the following error message:

  ```
  ERROR (dfw): Unknown group id: 21
  ```

  PR1592096
- xSTP might not get configured when enabled on a interface with SP style configuration on all platforms. PR1592264
- On the EX4400 chassis supporting POE, the `show poe controller` command might not show details of any POE firmware available for upgrade. You must manually perform a POE firmware upgrade during downtime to upgrade to the latest firmware if packaged with current software version installed on the device. PR1598766

High Availability (HA) and Resiliency

- The ksyncd core file might be observed while applying the configuration to a logical interface. PR1551777

Infrastructure

- On the EX4300 Virtual Chassis or Virtual Chassis Fan, HEAP malloc(0) is detected. PR1546036
- Traffic related to IRB interface might be dropped when mac-persistence-timer expires. PR1557229
- Traffic might not be forwarded on EX3400 and EX4300mp platforms with Layer 2 classifier rules applied. PR1561263
- Some MAC addresses might not be aged out on EX4300 platforms. PR1579293

Interfaces and Chassis

- The ppmd might crash when VRRP is configured on all Junos OS or EVO platforms. PR1561281
- MC-AE interfaces might go down if same VRRP group-id is configured on multiple IRB units. PR1575779
- The aggregate Ethernet interface might flap. PR1576533
- VRRP incorrect advertisement threshold values are seen on VRRP groups when VRRP is configured on EX2300 boxes. PR1584499

Layer 2 Ethernet Services

- An aggregated Ethernet interface flap might be seen during NSSU. PR1551925
- The DHCP client will be offline for 120 seconds after sending the DHCPINFORM message in the DHCP relay scenario. PR1575740

Layer 2 Features

- MAC addresses learnt from MC-LAG client device might keep flapping between the ICL interface. MC-AE interface after one child link is disabled. PR1582473

Platform and Infrastructure

- On the EX3400 Virtula Chassis, you cannot perform console access on the backup Virtual Chassis member. PR1530106

- Packets transiting through multicast-based VXLAN VTEP interface might be dropped post FPC restart. PR1536364
- The targeted-broadcast feature might send out duplicate packets. PR1553070
- The traffic might be dropped on Layer 3 LAG after rebooting or halting any member of EX4300 VC. PR1556124
- The LLDP neighbor advertisement on EX4300 might send an incorrect 802.3 power format with TLV length 7 instead of length Layer 2. PR1563105
- The last flapped timestamp for interface fxp0 resets every time when you perform `monitor traffic interface fxp0`. PR1564323
- When you enable the soft error recovery feature on Packet Forwarding Engine, the PFEX might crash. PR1567515
- On all EX9200 platforms with EVPN-VXLAN configured, the next-hop memory leak in MX Series ASIC occurs when a route churn for remote MAC-IP entries learned bound to the IRB interface in EVPN-VXLAN routing instance. When the ASIC's next-hop memory partition is exhausted, the FPC might reboot. PR1571439
- Introduce two new major CMERRORs for XM chip-based line card to stabilize the running device. PR1574631
- DHCP packets with source IP as link-local address drop in EX4300. PR1576022
- Firewall filter is not programmed correctly and traffic would be dropped unexpectedly. PR1586433
- The egress RACL firewall filter might not get programmed correctly on EX4300 platforms. PR1595797

Routing Protocols

- The ppmd memory leak might cause traffic loss. PR1561850
- The rpd process might crash if there are more routes changed during the commit-sync processing window. PR1565814
- The untagged packets might not work on EX Series platforms. PR1568533
- BGP session carrying VPNv4 prefix with IPv6 next-hop might be dropped. PR1580578
- The rpd might crash in scaled routing instances scenario. PR1590638

User Interface and Configuration

- The J-Web application cannot be auto-updated for all the supported EX Series devices. PR1563588

Virtual Chassis

- On the EX4600 and the EX4300 line of switches mixed Virtual Chassis, the following error message appears when you change the configuration related to interface:

```
'ex_bcm_pic_eth_uint8_set
```

  PR1573173

- EX4300 VCP might not come up after upgrade when QSFP+-40G-SR4/QSFP+-40G-LR4/QSFP +40GE-LX4 is used. PR1579430

Documentation Updates

There are no errata and changes in Junos OS Release 21.2R1 for the EX Series documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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 19,4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.1.

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.

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

Junos OS Release Notes for JRR Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 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

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for JRR Series Route Reflectors.

What's New in 21.2R1

There are no new features or enhancements to existing features for JRR Series Route Reflectors in Junos OS Release 21.2R1.

What's Changed

IN THIS SECTION

Learn about what changed in Junos OS main and maintenance releases for JRR Series Route Reflectors.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for JRR Series.

Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 21.2R1 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

Learn about open issues in this release 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.

There are no open issues for JRR Series in Junos OS 21.2R1 Release.

Resolved Issues

IN THIS SECTION

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: 21.2R1

IN THIS SECTION

Platform and Infrastructure

- On the JRR200 devices, the option-60 (Vendor-Class-Identifier) are not sent during ZTP. PR1582038

Documentation Updates

There are no errata and changes in Junos OS Release 21.2R1 for the JRR documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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 19,4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.1.

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.

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

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 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

Learn about new features or enhancements to existing features in this release for Juniper Secure Connect.

What's New in 21.2R1

There are no new features or enhancements to existing features for Juniper Secure Connect in Junos OS Release 21.2R1.

What's Changed

IN THIS SECTION

Learn about what changed in Junos OS main and maintenance releases for Juniper Secure Connect.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for Juniper Secure Connect.

Known Limitations

There are no known limitations for Juniper Secure Connect in Junos OS Release 21.2R1.

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 for Juniper Secure Connect in Junos OS Release 21.2R1.

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

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R1

There are no resolved issues for Juniper Secure Connect in Junos OS Release 21.2R1.

Documentation Updates

There are no errata and changes in Junos OS Release 21.2R1 for the Juniper Secure Connect documentation.

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 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

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for Junos fusion for enterprise.

What's New in 21.2R1

There are no new features or enhancements to existing features for Junos fusion for enterprise in Junos OS Release 21.2R1.

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for Junos fusion for enterprise.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for Junos fusion for enterprise.

Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 21.2R1 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 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

IN THIS SECTION

Learn which issues were resolved 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.

Resolved Issues: 21.2R1

There are no resolved issues in the Junos OS 21.2R1 release for Junos fusion for enterprise.

Documentation Updates

There are no errata and changes in Junos OS Release 21.2R1 for the Junos Fusion for enterprise documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

These release notes accompany Junos OS Release 21.2R2 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

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for Junos Fusion for Provider Edge.

What's New in 21.2R1

There are no new features or enhancements to existing features for Junos fusion for provider edge in Junos OS Release 21.2R1.

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for Junos Fusion for provider edge.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for Junos fusion for provider edge.

Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 21.2R2 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 open issues in the Junos OS Release 21.2R2 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

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R1

There are no fixed issues in the Junos OS Release 21.2R1 for Junos fusion for provider edge.

Documentation Updates

There are no errata or changes in Junos OS Release 21.2R2 documentation for Junos fusion for provider edge.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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 21.2R2 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/jinstall64-21.2R2.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.2R2.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/jinstall64-21.2R2.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.2R2.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 21.2R2 `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 21.2R2, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 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 from Junos OS Release 21.2

To downgrade from Release 21.2 to another supported release, follow the procedure for upgrading, but replace the 21.2 `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

These release notes accompany Junos OS Release 21.2R1 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

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

What's New in 21.2R1

IN THIS SECTION

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

Hardware

- The following methods to protect the chassis from excessive current draw and temperature conditions are supported:
  - Configure Junos OS to automatically shut down the PSM, or raise an alarm and log the event when a field-effect transistor (FET) failure is detected in the power supply module (PSM) by using the specified command. [See thermal-health-check].
  - Configure upgrade of the PSM firmware that will take actionwhen there is an FET failure by using the specified command. [See request system firmware upgrade].
  - Configure Junos OS to raise an alarm and log events when a PSM with upgraded firmware version shuts down due to an FET failure, Junos OS on the attached device.
  - Configure a monitor to check how much power the chassis draws from the PSM using the specified command. If the system draws more power from the PSM than what it should consume, Junos OS raises an alarm or shuts down the system. [See watchdog (PSM)].
    [See Handling Thermal Health Events Using Thermal Health Check and PSM Watchdog].

- **Support for QSFP-100G-FR transceivers (MX2010 and MX2020 with MPC9E and MIC-MRATE)**—Starting in Junos OS Release 21.2R1, the MX2010 and MX2020 routers with the MPC9E+MIC-MRATE support the QSFP-100G-FR transceivers.

  [See Hardware Compatibility Tool.]

- **Support for QSFP-100G-LR transceivers (MX2010 and MX2020 with MPC9E and MIC-MRATE)**—Starting in Junos OS Release 21.2R1, the MX2010 and MX2020 routers with the MPC9E+MIC-MRATE support the QSFP-100G-LR transceivers.

  [See Hardware Compatibility Tool.]

- **Support for QSFP-100G-FR transceivers (MX2010 and MX2020 with MX2K-MPC9E and MIC-MACSEC-MRATE)**—Starting in Junos OS Release 21.2R1, the MX2010 and MX2020 routers with the MPC9E+MIC-MACSEC-MRATE support the QSFP-100G-FR transceivers.

  [See Hardware Compatibility Tool.]

- **Support for QSFP-100G-LR transceivers (MX2010 and MX2020 with MPC9E and MIC-MACSEC-MRATE)**—Starting in Junos OS Release 21.2R1, the MX2010 and MX2020 routers with the MPC9E +MIC-MACSEC-MRATE support the QSFP-100G-LR transceivers.

  [See Hardware Compatibility Tool.]

- **Support for the JNP-SFP-10G-BX10D and JNP-SFP-10G-BX10U transceivers (MX10003)**—Starting in Junos OS Release 21.2R1, the MX10003 routers support the JNP-SFP-10G-BX10D and JNP-SFP-10G-BX10U transceivers.

  [See Hardware Compatibility Tool.]

- **Support for QSFP-100G-LR transceivers (MX240, MX480, and MX960 with MPC7E-MRATE)**—Starting in Junos OS Release 21.2R1, the MX240, MX480, and MX960 routers with the MPC7E-MRATE support the QSFP-100G-LR transceivers.

  [See Hardware Compatibility Tool.]

- **Support for QSFP-100G-FR transceivers (MX240, MX480, and MX960 with MPC7E-MRATE)**—Starting in Junos OS Release 21.2R1, the MX240, MX480, and MX960 routers with the MPC7E-MRATE support the QSFP-100G-FR transceivers.

  [See Hardware Compatibility Tool.]

Authentication and Access Control

- **802.1X authentication on trunk ports (MX Series)**—Starting with Junos OS Release 21.2R1, you can enable 802.1X authentication on trunk ports. We support authentication on the trunk port only in single supplicant and single-secure supplicant modes.

[See 802.1X Authentication on Trunk Ports.]

Flow-Based and Packet-Based Processing

- **Carrier-grade NAT (CGNAT) J-Flow logging (MX240, MX480, and MX960 with MX-SPC3 card)**—Starting in Junos OS Release 21.2R1, we've enhanced NAT logging using J-Flow version 9 and IPFIX format to generate logs. While creating or deleting events in NAT44 or NAT64 sessions, `jflow-logs` are generated.

  [See Understanding NAT Event Logging in Flow Monitoring Format on an MX Series Router or NFX250.]

High Availability

- **Unified ISSU with enhanced mode support (MX2008, MX2010, and MX2020 with MPC11E)**—Starting in Junos OS Release 21.2R1, we support unified in-service software upgrade (ISSU) in enhanced mode. Enhanced mode runs a second copy of the Junos OS software in standby mode. The second copy is ready to take over when the software updates the old image to a new one. Enhanced mode reduces packet loss to near-zero during the ISSU process.

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

  [See How to Use Unified ISSU with Enhanced Mode.]

- **NSR support for RSVP-TE dynamic tunnels (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support nonstop active routing (NSR) for RSVP-Traffic Engineering (RSVP-TE) dynamic tunnels.

  [See Nonstop Active Routing Concepts.]

- **Distributed and Inline BFD support for IPv6 link-local address (MX240, MX480, and MX960)**—Starting in Junos OS 21.2R1, we support distribution of OSPFv3 and ISIS BFD sessions which use IPv6 link local address. To forward packets with link local ipv6 address as destination from micro-kernel, we provide next-hop id as part of the packet which the PFE uses to forward the packet on right interface. Also, we support inline mode and by default the IPv6 Link local BFD sessions will operate in inline mode. This feature is supported on MX Series MPCs 1 to 9. This is not supported on MX Series MPCs 10 and 11.

  [See Understanding Distributed BFD.]

Interfaces

- **Support for VLAN rewrite operations on CCC interfaces (MX480 and MX960)**—Starting in Junos OS Release 21.2R1, you can configure VLAN rewrite operations on CCC interfaces.

  [See Configuring Q-in-Q Tunneling and VLAN Q-in-Q Tunneling and VLAN Translation.]

- **Support for coexistence of source IP hash with consistent hash (MX Series)**—Starting in Junos OS Release 21.2R1, source IP hash, which allows the flow from a particular source IP to always be hashed to the same link while load-balancing the flows across multiple paths, supports consistent hash, which prevents the reordering of flows to active paths in an ECMP group when one or more paths fail.

  NOTE: This feature is applicable only to external BGP (EBGP) ECMP paths.

  [See Configuring Load Balancing Using Source or Destination IP Only and Configuring Consistent Load Balancing for ECMP Groups.]

- **AMS on MPC10E line card (MX240, MX480, and MX960 with MX-SPC3)**—Starting in Junos OS Release 21.2R1, we support load balancing and high availability (HA) features on aggregated multiservices (AMS) interfaces for Layer 4 and Layer 7 services such as stateful firewall, intrusion detection service (IDS), and the Traffic Load Balancer (TLB) application.

Juniper Extension Toolkit (JET)

- **JET API support for GRE tunneling (MX204, MX240, MX480, MX960, MX2010, MX2020, and MX10003 with MPC1-MPC9E, MPC10E, or MPC11E; and VMX)**—Starting in Junos OS Release 21.2R1, we have enhanced Juniper Extension Toolkit (JET) APIs to support GRE tunneling and packet translation between IPv6 and IPv4. With the RIB (also known as routing table) service API and flexible tunnel profile API, you can embed GRE encapsulation and translation profiles. With the flexible tunnel service API, you can embed GRE de-encapsulation profiles.

  [See JET APIs on Juniper EngNet.]

- **BGP route service API supports programming routes with IP-IP encapsulation attributes (MX240, MX480, MX960, PTX1000, QFX5110, QFX5200, QFX10002, and QFX10008)**—Starting in Junos OS Release 21.2R1, you can use the BGP route service API to program BGP routes with IP over IP (IP-IP) encapsulation attributes. You can specify the tunnel type, the remote endpoint address, and the color of the route. Keep the following in mind:

  - The egress endpoint must be a unicast IPv4 address.
  - The colors encoded in tunnel_encap and extended_community must match.

- If the encapsulation ext_com and the tunnel attribute are both present, the egress endpoint must match the next-hop address.

To enable this feature, configure the `bgp-signal` option at the `[edit routing-options dynamic-tunnels tunnel-name]` hierarchy level. The rest of your dynamic tunnel CLI configuration does affect the functionality of the programmed tunnels.

[See dynamic-tunnels and JET APIs on Juniper EngNet.]

Junos Telemetry Interface

NOTE: For Routing Engine telemetry sensors supported by this platform, see Telemetry Sensor Explorer. If any Platform Forwarding Engine sensors have been added for this release, they are listed below

- **End-of-message notification for Routing Engine sensors (EX2300, EX4300, EX4300-MP, EX9200, MX240, MX960, MX10016, MX2010, MX2020, PTX1000, PTX3000, PTX10001, QFX5100, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we've introduced an end-of-message (EoM) Boolean flag for all Junos telemetry interface (JTI) Routing Engine sensors. The flag notifies the collector that the current wrap has completed for a particular sensor path. A wrap is a complete key-value data dump for all the leaves under a sensor path.

  The EoM flag also enables the collector to detect when the end of wrap occurs without having to compare stream creation timestamp values that the collector receives from the packets. Comparing timestamp values is costly time-wise and delays data aggregation.

  To use this feature with gRPC Network Management Interface (gNMI) transport or Remote Procedure Call (gRPC), retrieve the protobuf files from the relevant branch on the Juniper Networks download site:

  - GnmiJuniperTelemetryHeaderExtension.proto (gNMI)
  - agent.proto (for gRPC)

  For example: https://github.com/Juniper/telemetry/blob/master/20.3/20.3R1/protos/GnmiJuniperTelemetryHeaderExtension.proto.

  After you download and install the new protobuf files on a collector, the EoM field is present in the packets received.

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

- **CoS sensor support (MX204, MX240, MX960, MX2010, MX2020, MX10003, MX10008, MX10016, MX-ELM and vMX)**

Starting in Junos OS Release 21.2R1, we support the following streaming sensors with Junos telemetry interface (JTI).

- Interface queue extended statistics Packet Forwarding Engine sensors supported with Remote Procedure Call (gRPC): **/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**, and **/interfaces/interface/state/counters/out-queue/queued-bytes**.
- CoS interface set description Routing Engine sensor supported with gRPC: **/qos/interfaces/interface/state/interface-id**.
- Forwarding class to queue mapping Routing Engine sensors supported with gRPC: **/qos/forwarding-groups/forwarding-group/state/name** and **/qos/forwarding-groups/forwarding-group/state/output-queue**.
- Interface extended statistics sensor with native (UDP) support: **/junos/system/linecard/interface/queue/extended-stats/**.

[See sensor (Junos Telemetry Interface) and Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface)].

- **JTI: logical interface statistics for IPv4 and IPv6 family input and output counters (MX Series and PTX Series routers using third-generation FPCs)**—Starting in Junos OS Release 21.2R1, you can stream per-family logical interface statistics for IPv4 and IPv6 traffic using Junos telemetry interface (JTI) and Remote Procedure Calls (gRPC) to an outside collector.

  To access these sensors, use the resource paths **/junos/system/linecard/interface/logical/family/ipv4/usage/** and **/junos/system/linecard/interface/logical/family/ipv6/usage/** in a subscription.

  [See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).]

Layer 2 VPN

- **Support for Layer 2 services on SR-TE tunnels using transport class (MX series, PTX Series, and vMX)**—Starting in Junos OS Release 21.2R1, you can configure the following Layer 2 services on colored and non-colored segment routing traffic engineer (SR-TE) tunnels using transport classes.
  - Layer 2 Circuits
  - Layer 2 VPN
  - BGP VPLS

  [See Layer 2 Circuit Overview ,**Introduction to Configuring Layer 2 VPNs**, and BGP Classful Transport Planes Overview .]

MACsec

- **MACsec with GRES and NSR (MX140 and MX480 with the MIC-3D-20GE-SFP-E, MIC-3D-20GE-SFP-EH, and MIC-MACSEC-20GE line cards)**—Starting in Junos OS Release 21.2R1, Media Access Control Security (MACsec) support includes GRES and nonstop active routing (NSR) to provide nonstop MACsec service during a Routing Engine switchover.

  [See Configuring Media Access Control Security (MACsec) on Routers.]

MPLS

- **Support for the EVPN-LAN and P2P services using an MPLS-based core with IPv6 underlay (MX Series)**—Starting in Junos OS Release 21.2R1, we extend support for the EVPN-VXLAN and point-to-point (P2P) services using an MPLS-based IPv6 underlay. The services operate over an MPLS-based core with IPv6 addresses on the PE routers using Segment Routing with Multiprotocol Label Switching (SR-MPLS). The services also operate on the segment routing–traffic engineering (SR-TE) addresses that are responsible for the path calculation between the EVPN PE devices. You can use the EVPN-MPLS commands with the MPLS-based IPv6 underlays.

  To enable EVPN-MPLS-over-IPv6 functionality, set the `protocols evpn encapsulation mpls-inet6` configuration statement for each EVPN routing-instance in the `[routing-instances <routing-instance-name> protocols evpn encapsulation]` hierarchy level.

  [See Understanding EVPN with VXLAN Data Plane Encapsulation and protocols evpn encapsulation mpls-inet6.]

- **RSVP signaling over IS-IS nonforwarding adjacency (MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, you can configure any Level 1-Level 2 (L1-L2) routers that have been configured as a flood-reflector client to expand the flood-reflector hops in the Explicit Route Objects (EROs) carried in the `Path` messages. This feature enables the L1-L2 routers to signal RSVP over IS-IS nonforwarding adjacency by expanding the flood-reflector hops in the EROs instead of propagating the `Path` messages over the UDP tunnels.

  To know how to configure the flood-reflector interfaces, see How to Configure Flood-Reflector Interfaces in IS-IS Networks.

  To expand the flood-reflector hops in EROs, use the `rsvp expand-flood-reflector-hop` configuration statement at the `[edit protocols]` hierarchy level.

  Using the `traceoptions (Protocols RSVP)` command with the `flag event` option, you can view the new trace messages in the file that is created.

  The `show ted database` and `show rsvp session` command outputs introduce the following additional information:

Command	New Output Field	Description
show ted database	Flood reflector client, cluster-id *<number>*	Displays flood-reflector related information on the TE links and the cluster ID that the you have connected at the client side.
	Flood reflector, cluster-id *<number>*	Displays flood-reflector related information on the TE links and the cluster ID that you have connected in the flood reflector.
show rsvp session	Explct hop *<ip-address>* expanded	Displays the specific hop in the EROs that has been expanded by the router.

[See How to Configure Flood-Reflector Interfaces in IS-IS Networks, show ted database, show rsvp session, and traceoptions (Protocols RSVP).]

- **RSVP-TE supports preempting secondary LSPs that are signaled but not active (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, you can preempt secondary LSPs that are signaled but not active and configure the hold priority of the secondary standby label-switched path (LSP) for RSVP-Traffic Engineering (RSVP-TE). This helps to bring up non-standby secondary path LSPs with higher setup priority which are not able to come-up because of bandwidth crunch. To configure the non-active hold priority value for a secondary standby path, use the `non-active-hold-priority` statement at the [`edit protocols mpls label-switched-path <lsp-name> secondary <path-name>`] hierarchy level. You can set the priority from 0 through 7, where 0 is the highest priority and 7 is the lowest.

- **Support for 128 primary paths per static segment routing LSP (MX Series and PTX Series)**—Starting in Junos OS 21.2R1, we've increased the maximum number of segment-list bindings to an LSP tunnel from 8 to 128, with not more than 1000 tunnels per system. A maximum of 128 primary paths are supported per static segment routing LSP.

  [See Static Segment Routing LSP Limitations.]

Network Address Translation (NAT)

- **IPv6 MTU for NAT64 and NAT464 traffic (MX240, MX480, and MX960 with the MX-SPC3 card)**—Starting in Junos OS Release 21.2R1, you can configure IPv6 MTU for NAT64 and NAT464 traffic using the `ipv6-mtu` option at the `[service-set nat-options]` hierarchy level.

  [See Stateful NAT64 Overview.]

Network Management and Monitoring

- **CFM CCM support on PS interfaces (MPC7E, MPC8E, MPC9E, MPC10E, and MPC11E line cards)**—Starting in Junos OS Release 21.2R1, we support connectivity fault management (CFM) continuity check messages (CCM) on PS interface part of EVPN. You can configure:

  - CCM for down maintenance association end points (MEPs), that are down, on the PS interface to monitor the Ethernet networks for connectivity faults.
  - Remote defect indication (RDI) for the CCM frame.
  - Action profile with action link down for the remote MEP to bring down the PS interface when connectivity is lost.
  - Ethernet link trace (ETH-LT) and loopback (ETH-LB) are supported on the CFM session.

  [See Ethernet OAM Connectivity Fault Management.]

- **OAM ping support for segment routing with IPv6 (SRv6) network programming (MX Series)**—Starting in Junos OS Release 21.2R1, you can perform the Operation, Administration, and Maintenance (OAM) ping operation for any SRv6 segment identifier (SID) whose behavior allows upper layer header processing for an applicable OAM payload.

  Because segment routing with IPv6 data plane (SRv6) adds only the new type-4 routing extension header, you can use the existing ICMPv6-based ping mechanisms for an SRv6 network to provide OAM support for SRv6. Ping with O-Flag (segment header) is not supported.

  [See ITU-T Y.1731 Ethernet Service OAM Overview and How to Enable SRv6 Network Programming in IS-IS Networks.]

- **Support for syslog over TLS (EX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, you can transport syslog (control plane) over Transport Layer Security (TLS) protocol. Encapsulating syslog over TLS allows you to:

  - Validate the remote destination (syslog server) before transmitting any sensitive syslog information. (Authentication)
  - Encrypt the syslog during the transport. (Encryption)
  - Verify that the data has not been modified or tampered with (Integrity)

  Before you enable this feature, ensure you:

  - Configure public key infrastructure (PKI) in Junos
  - Configure and load the digital certificates
  - Configure the remote destination (syslog server) that supports syslog over TLS

To enable transport of syslog (control plane) over TLS, use the `tls` statement at the [`edit system syslog host host-name transport`] hierarchy level.

- **Syslog support to replay events (MX Series)**—Starting in Junos OS Release 21.2R1, you can replay syslog events over gRPC. Configure the `last` *`minute`* statementat the `[edit system syslog grpc-replay]` hierarchy level to replay events. You can also filter events based on facility and priority. Use the `facility` statement to filter events according to facility, and use the `priority` statement to filter events according to the priority at the `[edit system syslog grpc-replay]` hierarchy level. You can use the `facility` and the `priority` options to filter replay or live events.

  [See grpc-replay.]

Platform and Infrastructure

- **New MX10K-LC480 line card (MX10008 and MX10016)** —Starting in Junos OS Release 21.2R1, we've a new MX10K-LC480 line card with 48 SFP/SFP+ ports. The MX10K-LC480 has two Packet Forwarding Engines, each providing a maximum bandwidth of up to 240 Gbps.

  You can configure the ports as 10-Gigabit Ethernet interfaces or 1-Gigabit Ethernet interfaces. By default, the ports are 10-Gigabit Ethernet interfaces.

  > **NOTE**: You must install the MX10K-LC480 line card in the MX10008 and MX10016 routers along with the front panel with filter.

  You can configure the speed at the PIC level or port level. Configure the port speed of the line card at the [`[set chassis fpc <fpc> pic <number> pic-mode <mode>]`] or [`[set chassis fpc <fpc> pic <number> port <number>]`] hierarchy.

  Benefits of MX10K-LC480 Line card

  - Low cost card
  - Interoperability with the existing JNP10K-LC1201 card

  For information about the software features support, see Protocols and Applications Supported by MX10K-LC480 for MX Series Routers.

Routing Options

- **Enhancements to prefix-limit and accepted-prefix-limit configuration statements, and updates to show bgp neighbor command (ACX1000, EX9200, MX Series, PTX5000, and QFX10002)**— Starting from Junos OS Release 21.2R1, the `prefix-limit` and `accepted-prefix-limit` configuration statements include the following options:

- drop-excess <*percentage*>—If you include the drop-excess <*percentage*> option and specify a percentage, the excess routes are dropped when the number of prefixes exceeds the specified percentage.

- hide-excess <*percentage*>—If you include the hide-excess <*percentage*> option and specify a percentage, the excess routes are hidden when the number of prefixes exceeds the specified percentage.

The show bgp neighbor command has been enhanced to display the following additional information:

- Count of prefixes that are dropped or hidden based on network layer reachability information (NLRI) when the maximum allowed prefixes threshold is exceeded.

- Alerts when a peer starts to drop or hide routes.

- Configuration details of the prefix-limit and accepted-prefix-limit configuration statements.

[See prefix-limit, accepted-prefix-limit, show bgp neighbor, and Multiprotocol BGP.]

- **Forwarding class counters support for flat-file-profile (MX Series and vMX)**—Starting in Junos OS Release 21.2R1, the flat-file-profile statement supports forwarding class counters. You can now switch from the ingress CoS queue counters configuration to the forwarding class counters configuration. To enable the forwarding class counters feature, configure the use-fc-ingress-stats statement at the [edit accounting-options flat-file-profile *profile-name*] hierarchy level.

  [See flat-file-profile (Accounting Options).]

Routing Policy and Firewall Filters

- **Enhanced firewall filter processing on MPC10E and MPC11E line cards (MX Series)**—Starting in Junos OS Release 21.2R1, MX Series routers evaluate the terms attached to a firewall filter in an optimized fashion, and the maximum number of terms per filter increases to 8000.

  [See Understanding Firewall Filter Match Conditions.]

- **TCP SYN cookie (MX480 and MX960 with SPC3 card)**—Starting in Junos OS Release 21.2R1, we support the TCP SYN cookie. You can configure syn-cookie for the TCP protocol for source and destination.

  [See Configuring Network Attack Protection With IDS Screens for Next Gen Services.]

Routing Protocols

- **Support for origin validation with BGP sharding (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, you can use origin validation with BGP sharding. You can configure rib-sharding with routing-options validation.

- **BMP with BGP sharding and update I/O (JRR Series, MX Series, PTX Series, and vMX)**—Starting in Junos OS Release 21.2R1, we support BGP Monitoring Protocol (BMP) with BGP sharding and update I/O in the multithreaded mode.

- **Basic MVPN support with BGP sharding (cRPD, JRR200, MX2020, PTX5000, and QFX10002)**—Starting in Junos OS 21.2R1, we support the basic multicast virtual private network (MVPN) functionalities with BGP sharding.

  NOTE: Sharding is not supported for the MVPN address family.

- **Support for BGP SR-TE policy advertisement and error handling (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, if the SDN controller cannot directly install SR-TE routes on non-Juniper Networks devices, the controller installs the BGP SR-TE policy on the route reflector, which forwards the SR-TE routes to non-Juniper devices.

  To advertise SR-TE policy to non-Juniper devices, define a BGP policy that includes the `family inet-srte` statement at the `[edit policy-options policy-statement term from protocol bgp]` hierarchy level.

  To push an unlabeled IP packet before other labels, include the `inet-color-append-explicit-null`statement at the `[edit protocols source-packet-routing]`hierarchy level.

- **Support for SRv6 network programming and Layer 3 Services over SRv6 in BGP (MX Series)**—Starting in Junos OS Release 21.2R1, you can configure BGP based Layer 3 service over SRv6 core. You can enable Layer 3 overlay services with BGP as control plane and SRv6 as dataplane. SRv6 network programming provides flexibility to leverage segment routing without deploying MPLS. Such networks depend only on the IPv6 headers and header extensions for transmitting data.

  To configure IPv4 VPN and IPv6 VPN service over SRv6 core, include the `end-dt4-sid sid` and the `end-dt6-sid sid` statements at the `[edit routing-instances routing-instance name protocols bgp source-packet-routing srv6 locator name]` hierarchy level.

  [See Understanding SRv6 Network Programming and Layer 3 Services over SRv6 in BGP.]

- **Support for BGP classful transport (CT) with underlying colored SRTE tunnels (MX Series and PTX Series with FPC-PTX-P1-A)**– Starting in Junos OS Release 21.2R1, BGP-CT can resolve service routes using the transport RIBs and compute the next-hop. Services currently supported over BGP-CT can also use the underlying SRTE colored tunnels for route resolution.

  To enable BGP CT service route resolution over underlying SRTE colored tunnels, include the `use-transport-class` statement at the `[edit protocols source-packet-routing]` hierarchy level.

  [See use-transport-class.]

- **Flexible algorithm inter-level leaking support for SRv6 and SR-MPLS in ISIS (ACX Series, MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support flexible algorithm inter-level

leaking for SRv6 and SR-MPLS in IS-IS. Also, we partially support TE-App RFC 8919 in its basic form and extends 6PE support for flexible algorithm.

Services Applications

- **Support for the Juniper Resiliency Interface (MX480, MX960, MX2010, MX2020 and vMX)**—Starting in Junos OS Release 21.2R1, you can use our new Juniper Resiliency Interface (JRI) to detect, correlate, and mitigate exceptions. JRI extends the inline monitoring services feature with Juniper-specific IPFIX information elements (IEs) for exception data and introduces the concept of an Observation Cloud, which is a set of Observation Domains. You can send the IPFIX packets to either an on-box or an off-box collector.

  - You configure JRI with the `exceptions`, `store`, and `traceoptions` statements at the `[edit system resiliency]` hierarchy level.
  - You configure which categories of PFE exceptions are reported to a particular inline-monitoring instance with the `exception-reporting inline-monitoring-instance` *`instance-name`* `category` *`category-name`* `statement at the [edit chassis fpc` *`name`* `pfe` *`name`*`]` hierarchy level.
  - You configure the Juniper-specific IEs with the `primary-data-record-fields` statement at the `[edit services inline-monitoring templates` *`template-name`*`]` hierarchy level.
  - You configure the Observation Cloud ID with the `observation-cloud-id` statement at the `[edit services inline-monitoring]` hierarchy level.

  [See Inline Monitoring Services Configuration.]

- **Support for Routing-Engine based traffic sampling (MX Series with MPC10E and MPC11E line cards)**—Starting in Junos OS Release 21.2R1, you can configure Routing-Engine based traffic sampling. Traffic sampling enables you to copy traffic to a line card that performs flow accounting while the router forwards the packet to its original destination. You configure either an input or output firewall filter with a matching term that contains the `then sample` statement. Routing-Engine based traffic sampling supports only the version 5 and version 8 formats for exporting flow records.

  [See Configuring Traffic Sampling on MX, M and T Series Routers.]

- **Support for translation and GRE tunneling in data center environment (MX Series Routers)**—Starting in Junos OS Release 21.2R1, as part of upgrading the customer network for PaaS services, we support enhancement to your enterprise edge routers (MX routers). You can configure your edge routers to enable translation (IPv4 to IPv6 and IPv6 to IPv4) and GRE tunneling of the translated packets through the Juniper Extension Toolkit (JET) APIs. The edge routers now provide access to a Private Link Service offered as Platform as a Service (PaaS), bypassing the data center gateways.

  [See show flexible-tunnels profile and show-route .]

- **Support for `any` firewall filter family and Layer 2 firewall filter families for inline monitoring services (MX Series with MPC10E and MPC11E line cards)**—Starting in Junos OS Release 21.2R1, you can configure the `any`, `bridge`, `ccc`, or `vpls` family firewall filter with the term action `inline-monitoring-instance` *`inline-monitoring-instance-name`*.

  [See Inline Monitoring Services Configuration.]

- **Support for inline NAT services (MX240, MX480, MX960, MX2010, and MX2020 with MPC10E and MX2K-MPC11E line cards)**—Starting with Junos OS Release 21.2R1, we support inline NAT services. We support the following features:

  - 1:1 static address mapping
  - Bidirectional mapping: source NAT for outbound traffic and destination NAT for inbound traffic
  - No limit on number of flows
  - Source, destination, and twice NAT
  - Source NAT44
  - Destination NAT44
  - Source NAT with Interface Style
  - Destination NAT with Interface Style
  - Inline NAT with VRF

  [See Inline NAT.]

- **Interoperability of MPC10E with MX-SPC3 for IPSec services steering (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.2R1, the MPC10E-15C-MRATE and MPC10E-10C-MRATE interoperates with the MX-SPC3 card to enable the packet forwarding path that steers packets to the MX- SPC3 card. The MPC10E line card can perform the ingress or the egress processing for IPSec services packets through the `st0` and `vms` interfaces, nexthops, and the routes programmed in the line card.

  [See MPC10E-15C-MRATE and MPC10E-10C-MRATE.]

- **Interoperability of MPC10E with MX-SPC3 to support TLB (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.2R1, the MPC10E-15C-MRATE and the MPC10E-10C-MRATE interoperates with the MX-SPC3 card to support traffic load balancing. Using the Traffic Load Balancer (TLB) application, you can distribute traffic among multiple servers in a server group and perform health checks to determine whether any servers should not receive traffic. TLB supports multiple VPN routing and forwarding instance (VRF) instances..

  [See Traffic Load Balancer Overview.]

- **Support for unidirectional session refreshing (MX Series routers with MS-MPCs and MX-SPC3 services card)**—Starting in Junos OS Release 21.2R1, we support unidirectional session refreshing.

  For a service set, you can configure unidirectional session refreshing for the in-zone and the out-zone.

  At the `[edit services service-set <service-set-name> service-set-options]` hierarchy level, you can enable unidirectional session forwarding for:

  - Input (in-zone), by configuring the statement `unidirectional-session-refreshing input`.
  - Output (out-zone), by configuring the statement `unidirectional-session-refreshing output`

  [See service-set-options.]

Software Defined Networking (SDN)

- **SLCs support new asymmetric profile, multiversion software interoperability, GRES, and fabric hardening (MX2010 and MX2020 with MX2K-MPC11E)**—Starting in Junos OS Release 21.2R1, Junos node slicing with sub line cards (SLCs) supports the following features:

  - A new asymmetric profile which supports assigning DRAM size of 9 GB or 17 GB to an SLC independent of the PFE subset assignments.
  - Multiversion Software Interoperability

    > **NOTE**: If you are using sub line cards, Junos OS node slicing in 21.2R1 is not multiversion interoperable with any earlier release of Junos OS, including 21.1R1. For a GNF in a node-sliced system that uses SLCs to run Junos OS 21.2R1, all other GNFs and BSYS on that system must also run 21.2R1.

  - Fabric hardening
  - GRES on BSYS and guest network functions (GNFs). SLCs also support handling failure of links between the server and Control Boards (CBs).

  The SLC feature enables you to configure logical partitions of the MPC11E line card and assign each partition to different guest network functions (GNFs) in an external server-based Junos node slicing setup.

  [See Configuring Sub Line Cards and Assigning Them to GNFs.]

Software Installation and Upgrade

- **Increased memory allocation for Junos VM (MX204)**—Starting in Junos OS Release 21.2R1, we support increased memory allocation for Junos VM. The available VM size options are default (16GB) and high (24GB). After you update the VM size, you must perform a system reboot using the `request vmhost reboot` statement.

  Before you increase the memory, please contact Juniper Networks technical support to know the use cases that we support. After the memory upgrade, if you want to downgrade the Junos OS image, revert the VM memory to `default` and perform a system reboot using the `request vmhost reboot` command.

  [See VM Host Overview.]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Static route resolution over SR-TE tunnel (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support static route resolution over segment routing–traffic engineered (SR-TE) colored and uncolored label-switched paths (LSPs). To enable this feature, configure the `spring-te-lsp-next-hop` statement at the `[edit routing-options static` *`destination`*`]` and `[edit routing-options rib` *`rib name`* `static` *`destination`*`]` hierarchy levels. The feature support extends towards static, DTM, BGP-SR-TE, and PCEP source types that are currently supported by Source Packet Routing in Networking–Traffic Engineering (SPRING-TE). If a source is not configured, by default, it takes the next hop as static.

  You must configure the `tunnel-tracking` statement at the `[edit protocols source-packet-routing]` hierarchy level to enable this feature. This feature enhances the accuracy of first-hop label-based tunnel status for SR-TE tunnels according to their route resolution.

  [See spring-te-lsp-next-hop and source-packet-routing.]

- **Express segments using SR-TE underlay (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we've introduced SR-TE underlay path support for express segments to enable end-to-end transport of segment routing–traffic engineered (SR-TE) label-switched paths (LSPs) for very large multi-domain networks. The path is automated using segment-set or template policies for uncolored or colored segment routing policies. The `rib-group` configuration is required to import addresses to inet.3 for colored segment routing policies. When the express segments underlay is colored SR-TE, you need to configure the `no-chained-composite-next-hop` statement at the `[edit protocols source-packet-routing]` hierarchy level for the express segment to install the correct flattened next hop.

  This feature has the following limitations:

  - When the express segments underlay is colored SR-TE, the express segment does not inherit the SR-TE LSP underlay attributes (SR-TE name, metric).

  - The `install-nexthop` option at the `[edit policy-options policy-statement policy-name term term-name then]` hierarchy level to filter a specific SR-TE LSP bu its name is not supported.

- Express segments do not consider the respective weights of the primary and secondary segment lists of SR-TE LSP. Secondary LSP segments can be preferred for traffic even when the primary segment is up.

[See Express Segment LSP Configuration.]

Subscriber Management and Services

- **Advanced services support for static subscribers (MX240, MX480, and MX960 with MS-MPCs)**—Starting in Junos OS Release 21.2R1, you can configure the `static-subscriber-application` statement at the `[edit services service-set-name service-set-options]` hierarchy level to attach advanced services, such as deep packet inspection (DPI), to the static subscriber. [See Configuring Subscriber-Aware and Application-Aware Traffic Treatment Overview and service-set (Subscriber-Aware).]

- **Support for Broadband Edge subscriber management and services (MX10008 and MX10016 with MX10K-LC2101 and MX10K-LC480)**—Starting in Junos OS Release 21.2R1, we support subscriber management and services. The line cards also support subscriber access, subscriber authentication, service activation, and deactivation.

  [See Subscriber Management Overview.]

- **Junos Multi-Access User Plane support for 5G user plane function (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 21.2R1, Junos Multi-Access User Plane supports routers functioning as user plane functions (UPFs) in accordance with 3GPP Release 15 CUPS architecture. This provides high-throughput 5G fixed and mobile wireless service in non-standalone (NSA) mode. This includes support for the following:

  - N3, N4, N6, and N9 interface support
  - Roaming through the N9 interface
  - GPRS tunneling protocol, user plane (GTP-U) tunneling to the control plane
  - QoS Flow ID (QFI) support for 5G QoS flows

  [See Junos Multi-Access User Plane Overview.]

- **Support for PWHT with VC type 11 (MX Series routers with MPC7E, MPC10E, MPC9E, or MPC11E line cards)**—Starting in Junos OS Release 21.2R1, you can configure a pseudowire headend termination (PWHT) interface on a service PE router with `ethernet-tcc` encapsulation on the interface. With this feature, the service PE router does not have to support TDM/SONET/SDH-encapsulated traffic coming from access-side customers. The IP-based point-to-point pseudowire—which is an LDP-signaled FEC 128 (virtual circuit (VC) type 11)—connects the service PE router to the access device that is connected to the access CE router.

You configure the pseudowire to terminate into a Layer 3 VPN instance or a global IP table. The service PE router uses ARP mediation to resolve Layer 2 addresses when different resolution protocols are used on either end of a circuit.

The feature supports IPv4 and IPv6 payloads, and unicast and multicast traffic.

[See Configuring a PWHT with VC 11 Type Support.]

System Management

- **Support for PTP over Ethernet and hybrid mode over LAG interfaces (MX240, MX480, and MX960)**—The MPC2E NG and MPC3E NG line cards support Precision Time Protocol (PTP) over Ethernet and hybrid mode over a link aggregation group (LAG).

  Limitations

  There could be some performance limitations during a switchover from the active line card to the secondary line card and vice versa in a multi-line card scenario because of hardware limitations.

  If an unsupported line card is configured as the primary or secondary interface, the configuration goes through, but an error message is displayed in the output of the show ptp slave/primary CLI command. You must configure only supported line cards (MPC5E and MPC6E) to avoid this issue.

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

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for MX Series routers.

What's Changed in Release 21.2R1

IN THIS SECTION

Class of Service (CoS)

- Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

EVPN

- **Support for displaying SVLBNH information**—You can now view shared VXLAN load balancing next hop (SVLBNH) information when you display the VXLAN tunnel endpoint information for a specified ESI and routing instance by using `show ethernet-switching vxlan-tunnel-end-point esi` *`esi-identifier`* `esi-identifier instance` *`instance`* `svlbnh` command.

- **Log messages are removed (MX Series)**—When PTP aggregate Ethernet primary is configured, and PTP Aggregate Ethernet secondary is not configured, the log message **Profiles are being modified** is removed.

General Routing

- **Commit checks against incorrect configuration of SLC values (MX2020 and MX2010)**—We have introduced commit checks against incorrect configuration of sub line cards (SLCs). While configuring SLCs, if you specify any incorrect values (for example, unsupported Packet Forwarding Engine ranges, CPU cores, or DRAM values), the configuration commit fails with an appropriate message to indicate the error.

  [See Configuring Sub Line Cards and Assigning Them to GNFs.]

- **Enhancement to the show chassis pic command**—You can now view additional information about the optics when you run the `show chassis pic` command. The output now displays the following additional field: MSA Version: Multi-source Agreements (MSA) version that the specified optics is compliant to. Values supported are: SFP+/SFP28—SFF-8472 (versions 9.3 - 12.3), QSFP+/QSFP28—SFF 8363 (versions 1.3 - 2.10), and QSFP-DD—CMIS 3.0, 4.0, 5.0. Previously, the show chassis pic command did not display this additional field.

  [See show chassis pic.]

- **Enhanced response to URR query or remove request (MX Series)**—When the control plane function sends a URR query or remove request, the Junos Multi-Access User Plane now sends the usage report in the modify response.

- **VLAN isolation disabled by default (MX480, MX960, MX2008, MX2010, and MX2020)**—For Junos node slicing, the internal control plane no longer isolates GNFs from each other by default. The internal network has sufficient bandwidth to accommodate GNFs without needing to isolate GNFs from each other. However, if you want to isolate the internal traffic of each GNF from all others, you must configure the `set chassis network-slices vlan-isolation` CLI configuration statement (which is applicable for all uses except with sub line cards) on all the Routing Engines of the BSYS and GNFs and then reboot the chassis. If you want to configure the sub line card feature, you must ensure that VLAN isolation is disabled. We have deprecated the configuration statement `no-vlan-isolation`.

  [See vlan-isolation.]

- **ISSU is not supported**—Unified in-service software upgrade (ISSU) is not supported when clock synchronization is configured for Precision Time Protocol (PTP) and Synchronous Ethernet.

High Availability

- **Inline Mode for IPv6 Link local BFD sessions (MX240, MX480, and MX960)**—Starting in Junos OS 21.2R1, if an IPv6 link-local BFD session is set up, the transmission and reception entries are distributed and by default operates in inline mode. Prior to Junos OS 21.2R1 release, the transmission and reception were handled by the Routing Engine.

Interfaces and Chassis

- **Blocking duplicate IP detection in the same routing instance (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, and SRX Series)**—Junos will no longer accept duplicate IPs between different logical interfaces in the same routing instance. Refer to the table mentioned in the topic inet

(interfaces). When you try to configure same IP on two logical interfaces inside same routing instance, the commit will be blocked with the error displayed as shown below:

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.2/24

[edit]
user@host# commit
commit complete

[edit]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 2.2.2.2/24

[edit]
user@host# commit
[edit interfaces ge-0/0/2 unit 0 family inet]
  'address 2.2.2.2/24'
     identical local address found on rt_inst [default], intfs [ge-0/0/2.0 and ge-0/0/1.0],
family [inet].
error: configuration check-out failed</screen-output>
```

[See inet(interfaces).]

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python op scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the device passes command-line arguments to a Python op script, it prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device prefixes a single hyphen (-) to all argument names.

  [See Declaring and Using Command-Line Arguments in Op Scripts.]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

  When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set`

refresh or set refresh-from configuration mode command, first configure the cert-file statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See request system scripts refresh-from and cert-file (Scripts).]

Layer 2 Ethernet Services

- **Active leasequery-based bulk leasequery (MX Series)**—The overrides always-write-option-82 and relay-option-82 circuit-id configurations at the [edit forwarding-options dhcp-relay] hierarchy level are not mandatory for active leasequery-based bulk leasequery. For earlier releases, the overrides always-write-option-82 and circuit-id configurations are mandatory for active leasequery-based bulk leasequery. For regular bulk leasequery between relay and server without any active leasequery, the overrides always-write-option-82 configurations are mandatory.

  [See bulk-leasequery (DHCP Relay Agent).]

Layer 2 Features

- **Link selection support for DHCP**—We have introduced the link-selection statement at the [edit forwarding-options dhcp-relay relay-option-82] hierarchy level, which allows DHCP relay to add suboption 5 to option 82. Suboption 5 allows DHCP proxy clients and relay agents to request an IP address for a specific subnet from a specific IP address range and scope.

  Prior to this release, the DHCP relay dropped packets during the renewal DHCP process and the DHCP server used the leaf's address as a destination to acknowledge the DHCP renewal message.

  [See relay-option-82.]

Network Management and Monitoring

- **Chef and Puppet support removed (EX Series except EX4400, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, Junos OS products that were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS. FreeBSD 12.x based Junos OS does not support installing existing Chef or Puppet packages.

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See Creating Action Scripts for YANG RPCs on Devices Running Junos OS and Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules.]

- **Changes to <commit> RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server's response for `<commit>` operations includes the following changes:

  - If a successful `<commit>` operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.

  - The NETCONF server response emits the `<source-daemon>` element as a child of the `<error-info>` element instead of the `<rpc-error>` element.

  - If you also configure the `flatten-commit-results` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server suppresses any `<commit-results>` XML subtree in the response and only emits an `<ok/>` or `<rpc-error>` element.

  [See Configuring RFC-Compliant NETCONF Sessions.]

- **Changes in contextEngineID for SNMPv3 INFORMS (PTX Series, QFX Series, ACX Series, EX Series, MX Series, and SRX Series)**—Now the contextEngineID of SNMPv3 INFORMS is set to the local engine-id of Junos devices. In earlier releases, the contextEngineID of SNMPv3 INFORMS was set to remote engine-id.

  [See SNMP MIBs and Traps Supported by Junos OS.]

- **Change in OID ifHighSpeed**—Now, the object identifier (OID) ifHighSpeed displays the negotiated speed once negotiation is completed. If the speed is not negotiated, ifHighSpeed displays the actual maximum speed of the interface. In earlier releases, ifHighSpeed always displayed the actual speed of the interface.

  [See SNMP MIBs and Traps Supported by Junos OS.]

Software Defined Networking (SDN)

- **VLAN isolation disabled by default (MX480, MX960, MX2008, MX2010, and MX2020)**—For Junos node slicing, the internal control plane no longer isolates GNFs from each other by default. The internal network has sufficient bandwidth to accommodate GNFs without needing to isolate GNFs from each other. However, if you want to isolate the internal traffic of each GNF from all others, you must configure the `set chassis network-slices vlan-isolation` CLI configuration statement (which is applicable for all uses except with sub line cards) on all the Routing Engines of the BSYS and GNFs and then reboot the chassis. If you want to configure the sub line card feature, you must ensure that VLAN isolation is disabled.

  We have deprecated the configuration statement `no-vlan-isolation`.

[See vlan-isolation.]

VPNs

View the traffic selector type for an IPsec tunnel (SRX Series and MX Series)—You can run the `show security ipsec security-associations detail` command to display the traffic selector type for a VPN. The command displays `proxy-id` or `traffic-selector` as a value for the `TS Type` output field based on your configuration.

[See show security ipsec security-associations.]

Known Limitations

IN THIS SECTION

Learn about known limitations 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.

General Routing

- RPD slips are noticed on MX104 for customers that have large configuration load on the box with multiple services enabled (for example, l2circuits, VPLS, L3VPN, firewall-filters configuration, SNMP-polling, and so on). The fFollowing should be considered to avoid RPD slips for longer time duration:

  Configure system config: delta-export, persist-groups-inheritance, fast-synchronize.

  Reduce configuration size.

  Remove any trace-options and reduce the logging pressure on the NAND-flash storage.

Analyse the load from processes such as snmpd, mib2d, pfed processes if you are running SNMP. PR1361250

- In case of SyncE signal loss, DPLL3 goes into holdover and still the DPLL1/SYNTH1 signal output will be driven to control board (CB). So we see the CB DPLL in locked state because of this INVALID QL is seen. The CLI output for current clock status is always taken from CB DPLL state, so we see the status as locked. This command output is as per design. This is a display issue but the functionality works fine. PR1509356
- LFM might flap during MX Virtual Chassis ISSU to and from this release. PR1516744
- When an image with the third party SDK upgrade (6.5.x) is installed, the CPU utilization might go up by around 5 percent. PR1534234
- PTP to PTP noise transfer is passing for impairments profile 400nsp-p_1Hz, but failing for profile 400nsp-p_0.1Hz and lower bandwidth profiles as well. PR1543982
- In cRPD, the CLI command to show system core files directly is not available. If there is a process crash or there are core files in cRPD, the user needs to log in to docker explicitly and check (periodically) /var/crash/ for any process crash or core file generation. This is a current limitation due to the absence of a CLI command to access /var/crash (of Docker) from cRPD. PR1546097
- sFlow egress sampling of MPLS packets is not supported on MX Series platforms. PR1556659
- `Resource deadlock avoided` message is observed during software addition. There is no functionality impact due to this message. PR1557468
- On MX Series platforms, TTL value reported by sFlow egress sampling is equal to the TTL prior to decrement, that is, sFlow at ingress and sFlow at egress report the same value of TTL. PR1559565
- The eODN feature supports up to 1000 SR-TE LSPs with 32000 express segment links in TED. PR1561947
- RPD core file is generated during device reboot and/or daemon restart time. Daemon recovers and there is no service impact on routing protocol usage. Because of this, feature usage reporting for scale based licensed features in routing area will not be reported. PR1567043
- Statistics for the traffic entering into the tunnel get incremented on the ingress FPC where traffic came in, and telemetry statistics get reported from ingress FPC. PR1567227
- 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 unified ISSU is started, it is expected that the FPC restart will not be triggered by the user. If this is done, the ISSU can be aborted and system can be in-correct state. PR1572851

- On MX Series routers, unified ISSU or upgrade with validate option might fail if there is too less disk space in /var/tmp/. It is recommended to clear out all log files and core files before initiating upgrade with validate option (that is, when you are not using no-validate option) or unified ISSU. It is better to clear all unwanted data using `request system storage cleanup` to cleanup all unwanted data. You must ensure there is at least 9 GB free space in var/tmp after copying vmhost package file to /var/tmp/. PR1582554

- To upgrade to Junos OS Release 21.2R1, you need to include the no-validate option when issuing the upgrade command.

  Junos OS releases prior to 20.4R1 do not support the no-validate option with unified ISSU. In order to upgrade from an older release to Junos OS Release 21.2R1 with unified ISSU, you must first upgrade to a release that supports the no-validate option for unified ISSU, such as 20.4R1. PR1568757

Infrastructure

- Image validation fails with the following message: `mgd core @ _rs_init, _rs_stir, _rs_stir_if_needed`. PR1568757

MPLS

- Rpd process might crash after network service configuration changed (example, range of MPLS labels) without rebooting all the Routing Engines (which is a system mandatory step). PR1461468

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

Platform and Infrastructure

- With sensor being subscribed via Junos Telemetry Interface (JTI), after the interface is deleted, deactivated, or disabled, the TCP connection is still established, and the `show agent sensors` command still shows the subscription. PR1477790

Open Issues

IN THIS SECTION

Learn about open issues 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.

Authentication and Access Control

- When the Secure Shell Protocol (SSH) user accesses the device with TACACS+ authentication, the SSH might crash. The SSH user cannot access the device when the issue happens. PR1601150

Class of Service (CoS)

- On MX Series platforms, deactivating and activating the target-mode using the `set chassis satellite-management fpc target-mode` statement will lead to a bad state at Packet Forwarding Engine where the extended port based IFLSET will not have any queues at all while it should have actually had the queues. This will lead to traffic disruption. PR1593059
- When running NETCONF or any such session and querying interface information in XML format and having such multiple sessions (around 50-60) continuously asking for interface information might cause the child mgd process to get stuck, and if more than one (at least 4-5) child mgd processes gets stuck, the mgd will stop functioning, which might cause any new configuration to not take effect. PR1599024
- On all Junos platforms with `per-unit-scheduler` support, when the `per-unit-scheduler` is configured on aggregate Ethernet interface, after cosd restart or NSR switchover, unbind or bind of scheduler over child interface of aggregate Ethernet might occur. In NSR switchover scenario, traffic loss might be seen. PR1599857
- On the MX platform with MPC or MIC based line cards, the Class-of-Service rewrite policy might not work if the rewrite rules is tied to CCC interfaces. PR1603909

EVPN

- In a Provider Backbone Bridging-Ethernet VPN (PBB-EVPN) environment, ARP suppression feature which is not supported by PBB might be enabled unexpectedly. This might cause MAC addresses of the remote CEs not to be learned and hence traffic loss might be seen. PR1529940
- On all Junos platforms with EVPN-VXLAN scenario, the number of MAC-IP binding counters might reach the limit when MAC-IP is moved between interfaces. Since MAC-IP counters are not decremented when entry is deleted due to this defect, repeated moves will result in a limit (default value is 1024) that will be reached even though there are a fewer entries. Meanwhile, traffic loss might be seen. PR1591264

- In an EVPN A/A ESI multihoming scenario with dynamic list next hop (DLNH) configured, when one of the multihomed CE-PE links goes down on remote MH-PEs, then traffic loss might be seen. PR1594326

Forwarding and Sampling

- Traffic drop is seen and filter does not hit as expected for match condition traffic class with flt statement configured. PR1573350
- On Junos platforms, the snmpwalk might not work for some logical interfaces if the interface filter name is the same for input list filters. PR1601761

General Routing

- When you issue a `show interface` command to check the interface details, the system will not check whether the interface name provided is valid or invalid. The system will not generate an error message if the interface name is invalid. PR1306191
- Source MAC and TTL values are not updated for routed multicast packets in EVPN-VXLAN. PR1346894
- The ping latency behavior is expected for host generated ICMP traffic due to the design of Packet Forwarding Engine queue polling the packets from ASIC. PR1380145
- This is a timing issue during the sxe interface bring up (with respect to i40e driver). This can be recovered by rebooting the complete board. PR1442249
- In a race condition, if a BGP route is resolved over the same prefix protocol next hop in a routing table that has routes of the prefix from different routing protocols, when the routes are flapping (firstly these routes are down and then up), the BGP route will be re-resolved, and then the rpd process crash might be seen. PR1458595
- VXLAN VNI (multicast learning) scaling, traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- Either static routes or implicit filters should be configured for forwarding DNS traffic to service PIC. It solves DNS packet looping issue. PR1468398
- On MPC7E, MPC8E, MPC9E, MPC10E, JNP10K-LC2101, and MX204/MX10003, syslog error `unable to set line-side lane config (err 30)` will occasionally appear. This is does not impact any service and can be ignored. PR1492162

- The `show pfe filter hw filter-name <filter name>` command fails to retrieve the Packet Forwarding Engine programming details of the filter. PR1495712
- On all junos platforms with BGP SR-TE (Spring-TE), the transit v4 traffic in SR topology might miss labels and might get dropped in first hop, when ingress is forwarding traffic. It might miss out all the labels except the last hop in the v4 traffic forwarded by NH interface. PR1505592
- On a fully scaled system where all the slices are utilized by different families of CLI filters, if we try to delete for one family and add/change for another family with a higher number of filter terms which requires either expansion of the filter or creation of a new filter, the Packet Forwarding Engine fails to add the new filter as we are getting messages out of sequence. That is, the add/change of filter is called earlier than the delete of another filter that will free up the slices. PR1512242
- A 35 seconds delay is added in reboot time from Junos OS release 20.2R1 compared to Junos OS release 19.4R2. PR1514364
- Active sensor check fails while checking the `show agent sensors | display xml` command. PR1516290
- LFM might flap during MX Virtual Chassis ISSU from this release. PR1516744
- On the MX Series platforms with NG-RE installed, after upgrading the Intel i40e-NVM firmware to version 6.01, the FRUs disconnection alarms might be seen along with traffic loss. Refer to the TSB17603 to upgrade Junos software and Intel i40e-NVM firmware. PR1529710
- FIPS mode is not supported. PR1530951
- Due to BRCM KBP issue route lookup might fail. Need to upgrade KBP to address this issue. PR1533513
- MACsec PIC stays offline in new primary after ISSU in GNF alone. PR1534225
- `Socket to sflowd closed` error comes up when the ukern socket to sflowd daemon (server) is closed. The error is rectified by itself as the client successfully reestablishes the connection in the subsequent attempts. When these errors are consistent, it indicates a communication issue between sflowd and the sFlow running on the FPC. PR1538863
- On EVPN VXLAN, vmcore files are seen on master and backup Routing Engine with Layer 2 and Layer 3 multicast configuration. PR1539259
- In a scaled MX2020 router, with `vrf localisation` enabled, 4 million next hop scale, 800,000 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 does not come online. Rebooting master and backup Routing Engine will help recover and get router back into stable state. PR1539305
- The `Heap malloc(0) detected for jnh_unilist_adaptive_add` error messages are seen on loading the configuration. No functional impact due to this error. PR1547240

- Hardware performance counters might not be correctly exported to the CLI when Packet Forwarding Engine's are disabled. This is purely a display issue and required a high priority clean-up. PR1547890
- 100G AOC from Innolight does not come up after multiple reboots. It recovers after enabling or disabling interface.PR1548525
- When the telemetry data for a node which is streamed is deleted during a network churn and the same node is being walked/rendered for the sensor, RPD might generate core dump file. This is a corner case where the rendering and deletion of a particular node has to happen at the same instance. This issue can occur only in case of a unstable network. PR1552816
- 5M DAC connected between QFX10002-60C and MX2010 does not link up. But with 1M and 3M DAC this interoperability works as expected. PR1555955
- `Resource deadlock avoided` messages observed. No functionality impacts are seen. PR1557468
- Packet Forwarding Engine on a sub-LC (SLC) could show training failure (TF) on one or more planes, after events on other SLC of the same line card or after events that affect complete system. PR1558008
- On the MX10008 routers, the GRE keepalive adjacency state is Down even though the GRE tunnel is in the Up state. PR1559200
- VE CE mesh groups are default mesh groups created for a given routing instance. On vlan/bridge-domain add, flood tokens and routes are created for both VE and CE mesh-group/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, so this would not be a major issue. PR1560588
- Due to a race condition, the `show multicast route extensive instance instance-name` command output can display the session status as invalid. Such an output is a cosmetic defect and not an indicative of a functional issue. PR1562387
- Interface hold time needs to be configured to avoid the additional interface flap. PR1562857
- In a rare scenario, SPMB does not reply during FPC online which is moved from SLC mode to full line card mode. The FPC gets stuck as the training is not complete. PR1563050
- FPC online or offline through pinhole is not working. PR1563315
- When SLC is reconfigured from asymmetric mode to symmetric mode in a single commit, it is possible that on some occasions, one of the SLC shows chassis connection as dropped state. The SLC will come online and no functional impact is seen. PR1564233
- Starting Junos OS release 21.1R1, Junos ships with python3 (python2 is no longer supported). In ZTP process, if a python script is being downloaded, please ensure the python script follows python3 syntax. Also, the python script had #!/usr/bin/python as the first line (that is, the path of the python

interpreter), the same needs to be changed to #!/usr/bin/python3 from Junos OS release 21.1R1. PR1565069

- The `show pfe statistics traffic` command shows incorrect output and will be disabled in future releases as the correct place to check these statistics is PFE/flow-based `show pfe statistic` command. PR1566065
- During the ingress processing we maintain separate counters for Layer 2 unicast, multicast, and broadcast as well as for unknown unicast. where as during egress processing we only maintain the logical interface level stats after the wan out. Hence at egress level output multicast counter always shows 0. PR1566436
- The chassisd logs are flooded with the `pic_create_ifname: 0/0/0 pic type F050 not supported` error messages for every port that is connected. This happens repeatedly in a few seconds. PR1566440
- The tunnel composite next hop (TCNH) entries are present because NSR is not supported for BGP static programmable routes. In backup, this leads to an extra reference count due to which the next hop is not getting freed. This will be fixed when NSR feature is fully supported for this feature. PR1566666
- With SLC scenarios, the filter actions with discard/reject/send-to-host leads to crash AFTD. PR1567313
- On all L2NG platforms, MAC address entries might be smaller in the MAC table than in the ARP table, this is because some of the MAC addresses are not relearned successfully after MAC address age timeout. This issue causes traffic loss for non-existing MAC entries. PR1567723
- Packet Forwarding Engine error message `Tunnel id: does not exist` can be seen while executing the `show dynamic-tunnel database statistics` command after deactivating routing-options dynamic-tunnel when you have a high scale of tunnels. This is just a transient error message and has no functional impact. The error can appear while tunnels are getting deleted and will not be displayed after all the tunnels are deleted. PR1568284
- In high availability mode, ICMP fragment drop messages are not seen. PR1569123
- BUM traffic replication over VTEP is sending out more packets than expected and there seems to be a loop also in the topology. PR1570689
- PDB pull or synchronization does not occur in new primary during unified ISSU. This is a timing issue and it is seen whenever ISSU is done from any of the previous releases to Junos OS Release 21.1 or later. PR1570841
- Copying files to /tmp/ causes a huge JTASK_SCHED_SLIP. Copy files to /var/tmp/ instead. PR1571214
- In very rare scenario for high availability cluster deployment, when it does redundancy group 0 (RG0) failover and at same time, if the control link is down, then it generates mib2d core file because the

master Routing Engine and secondary Routing Engine are out of syncing dcd.snmp_ix information. PR1571677

- On VM Host platforms with Next-Generation-Routing Engine, the physical management interface is virtualized and mapped to fxp0 interface in guest OS, eth0 and macvlan0@eth0 interface in host OS. Currently, IPv6 is enabled by default on eth0 and macvlan0@eth0 interface on host OS. During system bootup or the management interface coming up, the management interface (that is, eth0 and macvlan0@eth0 interface) on the host OS might respond to IPv6 neighbor discovery protocol packets. It might cause the upstream router to learn the MAC address of eth0 and macvlan0@eth0 interface instead of fxp0 interface in Junos. In certain deployments (based on the upstream router configurations), the upstream router might disable the access to fxp0 interface. PR1571753

- On all Junos platforms in a subscriber scenario, routes that use static subscriber demux or ge interfaces as qualified next hop might be stuck due to the `Destination address required` error message after GRES or unified ISSU. This might cause high CPU usage for rpd. The rpd process restarts itself and system recovers automatically. PR1572130

- On all Junos platforms, traffic loss might be observed due to a rare timing issue when performing frequent Interface Bridge Domain (IFBD) configuration modifications. This behavior is seen when the Packet Forwarding Engine receives out-of-order IFBD(s) from Routing Engine and might lead to the fxpc process crash and traffic drop. PR1572305

- On the MX series platforms with EVPN-VXLAN setup, ARP MAC move between local side and remote side or moving from a MAC-VRF table to the default switch table might cause DCPFE/FPC to crash. PR1572876

- The ksyncd process generates core file when we reboot node with EVPN VXLAN configurations. PR1574594

- After Junos OS upgrade, MAC address changes will be seen on MPC9E PIC1 interfaces. Static MAC configurations will be affected. PR1575009

- The child inactivity timeout is not set for custom ALG application. This does not impact any functionality. Only user defined custom ALG child timeout will not get affect and it would consider default timeout. PR1575183

- When the scheduler configuration is not applied to all 8 egress queues of an interface and one or more egress queues is having `buffer size remainder` configuration, the distribution of buffer to egress queues with buffer size remainder is not distributed correctly, which might lead to unexpected tail drops. PR1575798

- Max ports used is not getting displayed properly in the `show services nat pool pool-name detail` command output. PR1576398

- On MX10016 routers, when `Fan Tray 1 Fan x> Failed` alarm is cleared, `Fan/Blower OK` SNMP traps are generated for fan tray 0 [Fan 31 - 41] and fan tray 1 [Fan 11 - 41]. PR1576521

- With max number of logical interfaces (4000 GRE tunnels per Packet Forwarding Engine) with following configuration:

  1. family inet and associated source and destination for each tunnel.

  2. Configure `allow-fragmentation` statement on one endpoint of the tunnel and configure `reassemble-packets` on the other endpoint of the tunnel.

  With the above configuration, if you do `deactivate chassis fpc` *`slot`*, SLIP messages are observed. PR1581042

- On MX platforms, in a subscriber scenario with scaled around 32,000 connections, the replication daemon might generate core files or stop running, which results in failure on subscriber services on the new Routing Engine after the upgrade or GRES. PR1577085

- In an EVPN-VXLAN scenario with OSPF configured over the IRB, OSPF sessions might not get established due to connectivity issues. PR1577183

- In a fully loaded devices, at times, firewall programming fails due to scaled prefix configuration with more than 64800 entries. PR1581767

- Unable to process route entries between Routing Engine and FPC, it is due to incorrect operations of two internal threads in a race condition, resulting in a tight loop on code and high rpd process CPU usage. PR1582226

- On MX platforms with SPC3, traffic drop is observed in either of the cases:

  Case 1: when there is an ICMPv6 error message is sent to the Address Family Transition Router (AFTR) IP. The ICMP error can be triggered from the Packet Forwarding Engine or the intermediate node having the AFTR address as the destination address. Flow ICMP vector will not handle this error as the destination is of AFTR and this leads to looping.

  Case 2: When there is a normal IP-IP session opened instead of a DSLITE session in case of the server to client session establishment and upon force tunnel session close by session timeout configuration or session clear command on the tunnel session and also with a timing case. PR1582447

- USB boot with Junos OS 21.2 image will get stuck in windriver mode. PR1582592

- When VRF localisation is enabled, CE or access facing FPC might generate core file when aggregate interface configuration is added or changed. PR1583901

- Multicast EVPN-VXLAN instance is down since local VTEP logical interface is not associated to EVPN instance post deactivate or activate of routing instance. PR1584109

- If a BSYS Routing Engine switchover is triggered by simulating a kernel crash on a node-sliced platform, the FPCs or SLCs stay in present state while the related GNFs become unreachable. A

system reboot is required to resolve this issue. This issue is seen only on MX2020 platforms with the REMX2K-X8-128G Routing Engine. PR1584478

- During reboot in certain instances, the device might get into a state where Junos OS virtual machine hangs until the NMI is triggered and reboots fully. The system recovers after ~30 minutes. PR1584902
- CoS classifiers and rewrites are not supported on a logical tunnel (LT interface) with Ethernet-CCC or Ethernet-bridge encapsulation. The cosd process does not prevent a commit but then the classifiers/rewrites are not bound to the LT interface at Packet Forwarding Engine and hence does not work. PR1585374
- MX Series routers with MPC11E line card and scaled pseudowire headend termination (PWHT) configurations, transient traffic loss is seen during iterative enhanced mode ISSU. The loss is usually seen in second or third ISSU iteration and ranges from 40-90 seconds. No traffic loss is seen in first ISSU iteration. Line cards and Routing Engine are not rebooted between ISSU iterations. PR1586337
- With preserve statement ON and option c is used with BGP CT; the VPN CT stitching routes at ASBR if resolving over an SR-TE tunnel having single label; then the forwarding mpls.0 route programming will be incorrect on MX boxes. PR1586636
- MX Series routers with MX-SPC3 services card, in USF mode, NAT EIM mapping is getting created even for out to in FTP ALG child sessions. PR1587849
- MX Series routers with MX-SPC3 services card, in USF mode, with NAPT44, EIM, APP, and PCP configurations, show services session count on vms- interface is not as expected for FTP traffic initiated from public side. PR1588046
- Rpd core is seen at the `rt_iflnh_set_nhid`. Core is due to assertion caused by failure of hbt_insert for nhid belonging to a logical interface. It is seen that there is a duplicate entry present which causes the hbt_insert failure. PR1588128
- A cloud LED on the device indicates the phone home client states and device connectivity state with the cloud. When the grpc application is configured with non root user, then the cloud LED will not display any pattern related to day1 states. The LED pattern will still be displaying the previous day0 state as applicable. PR1589321
- Fabric training failure might be seen on Packet Forwarding Engine, when the Packet Forwarding Engine sees a fabric self ping error and later if FPC hosting that Packet Forwarding Engine is restarted due to CLI or any other reasons. PR1590054
- Minor transient traffic drop will be seen during MBB of RSVP LSP without `optimize-adaptive-teardown` statement. PR1590656
- On MX Series platforms with PTP feature enabled with phy-timestamping, frequent phydriver sync_state toggling occurs due to incorrect calculation of the Phytimestamp. PR1591667

- With warm standby being configured for an aggregated multiservices (AMS) interface, if switchover is performed for the specified warm standby AMS interface or crash occurs on the service PIC where the AMS member interfaces are present, the mobiled daemon might crash. The mobiled daemon will restart automatically and be self-recovered after crash. PR1592345

- On MX platforms with dual Routing Engines, with GRES enabled and in PTP hybrid mode, if using the building-integrated timing supply (BITS) interface from backup Routing Engine for clock recovery, that will not work. PR1592657

- On MX platforms with SPC3 used, if adding the PS interfaces on the Routing Engine after SPC3 is up and running, the packet from the PS interface is sent to SPC3 for services like NAT, SFW, IDS, and etc might be dropped by SPC3. PR1592706

- Base system (BSYS) to guest network function (GNF) chassisd connection might be temporarily disrupted when two MS-MPC line cards, which are assigned to GNF, are booting up at the same time. If GRES is configured, there might be a mastership switch between GNF Routing Engine 0 and Routing Engine 1. PR1591598

- There can be a routes mismatch among SPRING-TE routes on master and backup Routing Engine when specific conditions are met:

  - Restart routing is done on master-rpd.

  - There are BGP-SRTE tunnels present in SPRING-TE.

  This mismatch does not present problems, post-swtch-over and no service impact is seen. As a workaround, restart routing on the backup Routing Engine. PR1596095

- A rare and intermittent AFT crash is seen after performing back to back deactivate and activate interface actions. PR1596320

- When configuring interface associated with service set is changed, during handling of this configuration change, crash happens due to incorrect pointer typecasting. This crash is seen intermittently. PR1596578

- In the case of HMC failure, the packet drop might be seen if traffic is moving from one FPC to another FPC. PR1594244

- On a node sliced platform with MPC11E line card sliced into sub line cards, it is possible that the `aftd-trio[13014]: [Error] IF:IfdCfgMsg, ifd not found, ifdIndex:2399` syslog error message might appear, when GNF has configuration that does not pertain to its Packet Forwarding Engines. This message does not have any functional impact. PR1594816

- On MX platforms with Virtual Chassis, firmware upgrading might fail due to improper Trivial Network Protocol (TNP) server address, so the firmware will fail to be downloaded to MIC. PR1595693

- When `suspend-for` is configured and user frequently restarts dot1x-protocol in CLI will end up MACsec session being not recovered at all. This is because unable to send MACsec suspension messages within short interval and ends with no new SAK programmed in hardware. Due to this, traffic loss occurs permanently. To recover the affected port, deactivate and activate MACsec on the port. PR1596854

- Carrier-Grade Network Address Translation (CGNAT) MX SPC3 AMS warm-standby 1:1 redundancy problem with CLI CPU statistics lost data after PIC failover. The `show services service-sets cpu-usage` command does not display service sets show services sessions utilization. The output does not display session count, the rates, and CPU values. PR1596976

- On all MX Series platforms, changing configuration AMS 1:1 warm-standby to load-balance or deterministic NAT might generate vmcore file and traffic loss might be seen. PR1597386

- On all Junos platforms with EVPN-VXLAN environment, when MAC/IP is moved from one Ethernet segment identifier (ESI) to another ESI from the same peer, the withdraw route might not be sent to the remote Virtual Tunnel End Point (VTEP), only MAC withdraw route is sent to the remote VTEP. PR1597391

- NTF-agent is not compatible with latest version of OpenSSL 1.1.1. It uses OpenSSL 1.0.2. PR1597714

- When MPC10 and MPC11 FPC is coming up, cfmman process might generate core files in case platform shared memory initialization did not happen fine and it tries to access that for getting slot ID information. PR1597812

- On the MX10008 and MX10016 routers, back to back offline and online of multiple FPC multiple times might result into FPC stuck at announce offline state. PR1598102

- ALG traffic might be dropped when incoming packet contains `HTTP/` and `rn` characters in data or NAT slipstream packets. PR1598017

- On all platforms support Junos telemetry interface, when the `set services analytics export-profile xxx format gpb-sdm` and `set services analytics export-profile xxx transport tcp` are enabled on Routing Engine sensors, subscriber management related daemons (like, authd, bbe-smgd, bbe-statsd, jdhcpd, and smid) might continuously crash and core files are generated. PR1598351

- On MX platforms, the Compact Forwarding Engine Board (AFEB) might crash 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

- On MX platforms with MS-MPC and MS-PIC, the packet loop might be seen after receiving the PCP mapping request packets to service-set where PCP rule is not configured and the packet loop might cause high CPU utilization. PR1598720

- Chassis components name exported wrongly. PR1598816
- MX Series routers with 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 due 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
- Unified ISSU might result in FPC core, if the `fast-lookup-filter` statement is enabled. PR1599045
- The rpd process generates core file on the standby Routing Engine when all of the following conditions are met:

  1). BGP-SRTE policy tunnels are present.

  2). The rpd process restart is done on the master Routing Engine.

  3). NSR switchover is subsequently done. PR1599446
- On the MX10008 and MX10016 routers, continuous offline and online of FPC multiple times might result into an FPC restart at init state causing additional 2 min in boot time. PR1599469
- On MX SPC3 services card, ICMP protocol is not detected and does not allow user to modify inactivity-timeout values. PR1599603
- In a node sliced platform with MPC11E is being used in sub line card mode, if the configuration of the SLC is moved from asymmetric mode to symmetric mode followed by a swap of Packet Forwarding Engine range between SLC1 and SLC2, generates ukern-platformd and ztchip core files on some rare occasions. The line card will recover on its own and no functional impact will be seen once the line card is online. PR1600040
- On MX platforms with multiservices card (MS-PIC or MS-MPC) installed, when the user's TCP session is passing the multiservices card, TCP tickle functionality tries to extend TCP session after the inactivity timeout expires by sending self-generated TCP keepalive packets to both parts of TCP connection and expecting the TCP ACK to be seen from both parts. While the expected behavior is to drop that TCP ACK packet on multiservices card upon receiving, it sends to another part of TCP connection, this causes confusion and inability to extend TCP session, and then causes impact on long-lived TCP sessions with low volume of traffic. PR1600619
- Frame stack messages are seeing during MPC11E subLC boot up, when subLC is added to GNF. There is no functional impact is seen due to the messages. PR1600749
- On MX platforms with multiple MPC2E NG, MPC3E NG, and MPCE type 3 3D installed and working in redundant mode (some line cards just working as spare role), if you change the mode from `redundant` to `increased-bandwidth` (all line cards should be online without any spare role), one of the previous spare

line cards might not get online and stay in check status. That might cause traffic loss or performance degradation. PR1602080

- J-Flow syslog messages are seen when CGNAT is using 0x0000 in IPv4 identification field. This might causes issues for some J-Flow syslog collectors especially when J-Flow syslog packets get fragmented along the path to collector. PR1602528
- When inband management IRB interface is not assigned with IP address or there is no DNS configured on the device, the cloud LED will display the pattern for `NO_CLOUD_RESPONSE` state of instead of NO-IP-Addr or NO-DNS. PR1602664
- On MPC2E-3D-NG and MPC3E--3D-NG line cards with the certain chip set based MIC (like 20x1G MIC and 2x10G MIC), the Packet Forwarding Engine might be disabled while ungracefully removing the MIC from the MPC (for example, without taking the MIC offline using CLI or with a MIC button). PR1602939
- On the MX10008 and MX10016 routers, during Routing Engine switchover, if there is a burst of ICMP, BFD, SSH, FTP, TELNET, and RSVP packets (~18,000 pps), then the new backup Routing Engine might restart. PR1604299
- On MX150 platform, when the `hold-up` time is configured on an interface, if the interface goes from down to up, the up hold-time timer is triggered. But hold-time up does not work as the interface comes up immediately even the timer still does not expire. PR1604554
- On the MX10008 and MX10016 routers, when fabric plane goes offline and online might result in destination error on line cards. PR1605770
- On MX Series with MPCs/MICs based platforms working as MPLS transit router, if entropy label is configured and the ingress interfaces and egress interfaces of the LSP are on the same Packet Forwarding Engine, an extra entropy label might be pushed to the LSP. Traffic loss might be seen if the egress routers cannot handle the extra entropy label (for example, DPC to DPC connection on the egress router with the penultimate router). PR1605865
- On the MX10008 and MX10016 routers, when the FPC turns offline and online multiple times, FPC online operational command shows incorrect message and the FPC might remain offline. PR1607147
- In a subscriber management scenario, under a rare condition, the kernel might crash at very rare condition due to a null pointer check when an entry lookup is performed. PR1607282
- On the MX10008 and MX10016 routers, issues are seen when there is a Packet Forwarding Engine error causing disable-pfe, which is not seen in the normal FRR switchover. PR1609768
- On the MX10008 and MX10016 routers, the `show network agent` command output must be null, but which shows statistic per component after GRES. PR1610325

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. When ksyncd crashes on backup Routing Engine, a live kernel core file is also generated on both the Routing Engines. There is no service impact due to this issue. PR1606779

Infrastructure

- The `show system processes detail` CLI command does not display CPU details under the CPU column. PR1588150

Interfaces and Chassis

- On Junos platforms with VRRP failover-delay configured, changing VRRP mastership might cause peer device to relearn VIP ARP entry on old master interface due to timing issue. PR1578126
- On all Junos platforms, the dcd process crash might be seen after performing Routing Engine switchover or reboot of the device or management interface configuration change due to memory corruption triggered by a code in the Junos OS kernel. PR1587552
- On the MX platforms, the dcd internal data structure of the distribution bundle might get corrupt after removing the aggregated Ethernet logical interface of members of a targeted logical interface set from the targeted distribution database. Later, the dcd process crashes when it accesses the corrupted entry. PR1591032
- With aggregated multiservices interface (AMS) configured, the memory leak on dcd daemon occurs when making configuration changes on any interface. The leak rate is slow and depends on the scale of the logical interfaces on AMS interfaces (for example, if there are 8 AMS physical interfaces with 8000 logical interfaces, the leak is about 5 MB on each commit), which might lead to dcd crash. PR1608281

Juniper Extension Toolkit (JET)

- The stub creation functions will not be available. PR1580789

Layer 2 Ethernet Services

- On MX5, MX10, MX40, MX80, MX104 platforms with DHCP server configuration for DHCP subscribers, the jdhcpd memory leak might happen and the memory increase by 15 MB which depends on the number of subscribers when testing the DHCP subscribers log in or log out. PR1432162
- On MX platforms with DHCP ALQ, the Active Lease Query (ALQ) TCP queue might get stuck. This might cause the subscribers from backup BNG not to be able to sync with master BNG and eventually causing the subscribers in the master starts go down and result in a major outage. PR1590421
- The jdhcpd generates core file when dhcp process restarts and there is no service impacts. PR1594371

MPLS

- As the update-threshold configuration changes from an attribute to an object, you need to delete the update-threshold stanza and re-configure it after the downgrade. PR1546447
- The RSVP interface update threshold configuration syntax has changed between Junos OS Release 18.2X75-D435 and Junos OS Release 20.3X75-D10 to include curly braces around the threshold value. Upgrading and downgrading between these releases is not entirely automatic. The user must delete this stanza if configured before the downgrade and then manually reconfigure. PR1554744
- When some LSPs that request facility backup protection using bypass tunnels are brought up using respective Resv messages that do not contain the mandatory RECORD_ROUTE object. When such LSPs undergo local repair, then RPD process generates core file with the backtrace specified in this problem. If either the Resv messages originated by egress LERs contain the mandatory RECORD_ROUTE object or if such LSPs brought up with mal-formed Resv message does not undergo local repair, then the core file will not be generated. PR1560059
- Extended-admin-groups on links are shown as SRLG attribute in TED. PR1575060
- On the MX10008 and 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
- On all Junos platforms with NSR configured, when the `dual-tranport` is configured under protocols ldp and the inet-lsr-id and inet6-lsr-id is different from the router-id, the LDP replication session might not get synchronized and causing traffic loss during Routing Engine switchover. PR1598174

- When a protected link goes down, MPLS gets tunnel local repair message from RSVP and trigger CSPF computation. Next, MPLS gets link protection information through RRO notification. If MPLS receives TED notification first before RRO notification, then CSPF computation fails. Since the link protection flag is not set, MPLS thinks it is an unprotected link and brings down the LSP. PR1598207

- On all Junos platforms with NSR configured, if the `dual-transport` is configured under `protocols ldp` and the inet-lsr-id and inet6-lsr-id is different from the router-id, VPLS connection on peer device might get down and traffic loss might occur during Routing Engine switchover. PR1601854

- On the MX10008 and MX10016 routers, when there is scaled RSVP sessions (for example, 21,000) and RSVP is enabled for all the interfaces, the rpd process goes through all the interfaces which results into high CPU utilization for some time. This might also result in LSP flap, log messages on Routing Engine switchover, and protocol flap. PR1600159

- In an RSVP environment with `fast-reroute` enabled, when an LSR in a detour LSP goes down in particular scenario, the newly signaled detour path might be brought down and remain in incomplete state, due to a defect in RSVP-IO thread that it continues sending incorrect path refresh which brings down the detour path. PR1603613

- On the MX10008 and MX10016 routers, the `show route forwarding-table destination` *address* shows stale entry for ~60 sec. There is no traffic impact due to this. PR1610620

- The rpd process might crash on standby Routing Engine LDP module when VPLS mac-flush enabled on peer by default or configurared. The core files are generated only when the peer sends LDP. The address_withdrawal_message with first TLV other than address_tlv. This issue occurred particularly with extreme networks as peer VPLS PE. PR1610638

Network Management and Monitoring

- The SNMP polling failures timeout might be observed when the number of outstanding requests to any subagent (for example, mib2d, snmpd-subagent) reaches 500. This will impact the SNMP polling functionality. PR1585409

- When the ARP entry gets removed in the ARP table, and if there is a presence of a static route referring to the removed next hop IP, the refcount will not be 0. In that case, the kernel will not send a DELETE message to mib2d. As a result, SNMP still has the ARP entry even after it is expired in the ARP cache. PR1606600

Platform and Infrastructure

- MPLS traffic going through the ingress pre-classifier logic might not determine MPLS payload correctly, classifying MPLS packet into control queue versus non-control queue and exposing possible packet re-order. PR1010604
- On MX Series platforms with MPC7, MPC8, and MPC9 line card or MX-204 and MX-10003, when the packets which exceed the MTU and whose DF-bit is set go into a tunnel (such as GRE, LT), they might be dropped in the tunnel egress queue. PR1386350
- Loss of traffic on switchover when using filter applied on logical interface. PR1487937
- With GRES and NSR functionality with VXLAN feature, the convergence time might be slightly higher than expected for Layer 2 domain to Layer 3 VXLAN. PR1520626
- On MX Series routers, the blockpointer in the ktree is getting corrupted leading to core file generation. There is no functional impact such as FPC restart or system down. PR1525594
- When the DHCP relay mode is configured as no-snoop, we are observing that the offer gets dropped due to incorrect ASIC programing. PR1530160
- RPM behavior in non-delegate mode with MPC10 line cards: The RPM packets from client are received and processed by RPM server but the response packets are dropped before they are received by the client. PR1556697
- A buffer overflow vulnerability in the TCP/IP stack of Junos OS allows an attacker to send specific sequences of packets to the device thereby causing a Denial of Service (DoS). PR1557881
- On all MX platforms, the L2TP tunnel will not work with filter-based encapsulation for the breakout interface. This issue is seen as the parsing logic in Packet Forwarding Engine for getting the tunnel parameters could not handle breakout interface scenarios. PR1568324
- This issue might be seen only in back to back GRES in about more than 40 to 50 iterations. No workaround available and FPC gets restarted. PR1579182
- Ethernet-output-bytes are not in expected range while verifying Ethernet MAC level with both IPv4 and IPv6 traffic for VLAN tagged interfaces. The issue is due to output byte count not getting updated properly. The script log shows that there is no packet loss and there is no functional impact. PR1579797
- A buffer overflow vulnerability in the TCP/IP stack of Juniper Networks Junos OS allows an attacker to send specific sequences of packets to the device thereby causing a Denial of Service (DoS). PR1595649

- On platforms with both enterprise style and service provider style configurations, an interface with enterprise style logical interface and flexible-vlan-tagging configured, VLAN tagged traffic might be dropped due to incorrect programming in the system. PR1598251
- In an enhanced subscriber management environment, if a service filter is applied to a dynamic service set, the service filter instance will be created on Packet Forwarding Engine based on the configured service filter template. If the configured service filter template is changed at the same time a service filter instance is instantiated, the service filter might get incorrectly programmed in Packet Forwarding Engine due to a rare timing issue. This issue might cause the service failure. PR1598830
- When a Virtual Chassis is scaled with different feature configurations and device is stressed with traffic, device might not respond for CLI commands for a short period of time and a vmcore file might be reported at that time. Once VM core is saved, device will continue to operate normally. PR1599498
- On all Junos platforms with authentication-key-chain configured for BGP, if restarting BGP connections after deleting the authentication-key-chains, the kernel might crash. The deleted operation can be executed by the delete security authentication-key-chains command. PR1601492
- On MX platform working as PE in MVPN, when traffic is received (from core) on upstream multicast LSI interface and then forwarded over VPLS via IRB interface, the packets are forwarded without vlan-tags, which leads to traffic drop at the remote VPLS PE due to missing vlan-tags. PR1607311

Routing Policy and Firewall Filters

- The dns-name entries in policies might not be resolved if the routing instance is configured under a system name server. PR1539980

Routing Protocols

- While interoperating with other vendors in a draft-rosen multicast VPN, by default Junos OS attaches a route target to multicast distribution tree (MDT) subsequent address family identifier (SAFI) network layer reachability information (NLRI) route advertisements. But some vendors do not support attaching route targets to the MDT-SAFI route advertisements. In this case, the MDT-SAFI route advertisement without route-target extended communities are prevented from propagating if the BGP route-target filtering is enabled on the device running Junos OS. PR993870
- SCP command with routing option (-JU) is not supported. PR1364825

- On all platforms with a large-scale BGP setup (for example, advertising 300,000 routes over 500 BGP peers), high CPU utilization (close to 100 percent) by BGP I/O thread on master Routing Engine might be seen for a couple of minutes, which might lead to dramatic performance degradation and even traffic loss if NSR is enabled while there is a lot of advertisements and the backup Routing Engine is busy. PR1488984

- 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

- Routes are not copied from trasnport ribs (junos-rti-tc-200.inet.3) to bgp.transport.3 in device with transport family enabled. PR1556632

- A single hop BFD session over IRB interface works in centralised mode if the VPLS instance the IRB belongs to has only LSI interfaces bound to VPLS pseudowires and has no local non-tunnel attachment circuits. PR1563947

- On Virtual Chassis or Virtual Chassis fabric, inconsistent MCSNOOPD core file is seen when igmp-snooping configuration is removed. PR1569436

- If Junos OS configuration contains a SHA-1 hashed password for a specific user, that user will be unable to login post upgrade. To identify any SHA-1 hashed passwords, run the following from the edit mode: `show | match \$sha1\$`. The password format post upgrade is not SHA-1. If the password format is set to SHA-1, the password will be hashed with SHA-512 instead. PR1571179

- Multiple single-hop BGP sessions on different links using the same link-local address. PR1575179

- Traffic loss across the LDP path during traffic shift to another device in the MPLS cloud. Here two routers with two different capacities are converging at two different times, so the micro loop occurs between the two nodes. PR1577458

- The `use-for-shortcut` statement is meant to be used only in SR-TE tunnels which use Strict SPF Algo 1 (SSPF) 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 SR-TE tunnel using Algo 0 prefix SIDs is configured with the `use-for-shortcut` statement, it could lead to routing loops or rpd process core files. PR1578994

- On all Junos platforms, when a BGP peer flaps, if the received routes are changed by the BGP process from active to inactive while cleaning up these received routes, the rpd crash might be seen. PR1592123

- On all Junos platforms with OSPFv3 is used, if there are multiple router link-state advertisement (LSA) from the same peer, the rpd process might be stuck at 100 percent during the router LSAs update. PR1601187

- After changing MTU on an interface, BGP routes that are resolved over IS-IS will be installed in kernel as dead and traffic will drop. PR1605376

- On all Junos platforms, if both rib-sharding and 4-byte peer-as (AS number 65536 or greater) are configured, then BGP peers with 4-byte peer-as might flap whenever any configuration change occurs. PR1607777

Services Applications

- Core files has been generated at `kmd_gen_fill_sa_pair_sadb_flags @kmd_update_sa_in_kernel @kmd_sa_cfg_children_sa_free`. This is not a functional issue but can be seen when kmd is closing and final cleanup is happening. There are no functional impact as kmd is shutting down. PR1600750

Subscriber Access Management

- In a subscriber scenario, if RADIUS accounting backup is configured and the RADIUS server is unavailable for more than 30 minutes, some subscribers might be stuck in terminated state and cannot be recovered even if the RADIUS server is reachable. PR1600655

Unified Threat Management (UTM)

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

User Interface and Configuration

- When a user tries to deactivate the MPLS related configuration, the commit fails on backup Routing Engine. PR1519367
- Mgd process generates core file when executing image upgrade command. The issue can be avoided with a simple workaround by providing a valid package during upgrade command. PR1557628
- Core files are generated at cbsd_util.c:cbsd_db_open:203 along with load override. As a workaround use `load update` instead of `load override`. PR1569607
- When 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 will be seen. This will not have any impact on the running traffic. PR1599641

VPNs

- During unified ISSU, the IPsec tunnels flap, causing a disruption of traffic. The IPsec tunnels recover automatically after the ISSU process is completed. PR1416334
- In some scenario (for example, configuring firewall filter) sometimes routers might show obsolete IPsec SA and NHTB entry even when the peer tears down the tunnel. PR1432925
- In an MVPN scenario with ingress replication, selective provider tunnel is being used, if the `ink-protection` statement is added or deleted from the LSP for MVPN, rpd process might be crashed. The reason is that when `link-protection` is deleted, the ingress tunnel is not deleted, and when `link-protection` is added back, it tries to add same tunnel. Due to which, the rpd process asserts as same tunnel exists and the rpd generates core files. PR1469028
- Currently none of the export policies are applied to MVPN route types 4, 6, and 7. This was required to skip the vrf-target communities, not to be applied on these route types. However, if a vrf-export policy is applied on the VRF, then the operator must set the communities appropriately and this export policy should get applied to all routes in that VRF. With this change vrf-export policy will get applied to all MVPN route types. PR1589057
- In Next Generation Multicast VPN (NG-MVPN) with GRE as transport tunnel, the ddos-protection reason `Packets failed the multicast RPF check` is seen when mGRE packets flow is received from I-PMSI tunnel to mPE without active subscribers in C-multicast group, it does not look as a correct reason for DDoS violation. PR1591228

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R1

IN THIS SECTION

General Routing

- Revert of RLT to primary might silently discard traffic for around 10 minutes after the primary FPC is online with primary RLT up. PR1394026
- Unable to show to which shard a given route is hashed. PR1430460
- Configuring two IPsec gateways for V1 and V2, triggering IKEv1 client tunnels AutoVPN hub always checks with IKEv2 policy and not on IKEv1. PR1465970
- The following line card errors are seen: `HALP-trinity_nh_dynamic_mcast_add_irb_topo:3520 snooping-error: invlaid IRB topo/ IRB ifl zero in l2 nh 40495 add IRB`. PR1472222
- FPC might crash after performing unified ISSU on the device which equips the type of 3D 20x 1GE MIC. PR1480212
- Subscribing to /linecard/packet/usage and triggering the UDP decoder, the hardware statistics are exported with improper hierarchy. PR1485739
- Incorrect log message for PIC1 when changing the configuration from PIC mode to port mode. PR1500429
- Aggregate Ethernet interfaces do not display member link statistics. PR1505596
- MX150 routers might go into db mode after software upgrade or downgrade. PR1510892
- Sometimes external 1 pps cTE is slightly above Class B requirement of the ITU-T G.8273.2 specification. PR1514066
- On the MX960 routers, the `show interfaces redundancy rlt0` statement shows current status as primary down as FPC is still in the ready state after RLT failover (restart FPC). PR1518543
- Packet drops might be seen with all commit events when interface configured with 1 Gbps speed. PR1524614
- RADIUS framed route sent via RADIUS initiated COA message might not be installed into the routing table. PR1524628
- The aggregated Ethernet interface might not come up with LFM configured after reboot. PR1526283
- Removing superflous XML tags within syslog strings. PR1528116
- On MX150 routers, configuring the `no-flow-control` statement under gigether-options does not work. PR1531983
- Wavelength unlocked alarm is On when using SFP+-10G-T-DWDM-ZR optics. PR1532593

- On the Virtual Chassis and Virtual Chassis fan, after NSSU while performing GRES, backup can generate core file and go to the database prompt. PR1533874
- The dcpfe process might crash and cause FPC to restart due to the traffic burst. PR1534340
- The CFM sessions go down during FRU upgrade stage of unified ISSU in MX Virtual Chassis. PR1534628
- The spcd process might crash during early initialization. PR1535536
- Certain Linux based FPCs might reboot if TNP neighbor towards backup Routing Engine continuously flaps on dual Routing Engine platforms. PR1537869
- The following error message might be seen during upgrade of VM host platform: `vmhost-platform-grub-install.sh: line 140: [: ==: unary operator expected`. PR1537980
- On the AFT based FPCs (MPC10 and MPC11 line cards), the `show jnh exceptions inst` command of the Packet Forwarding Engine might cause the FPC process to crash. PR1538138
- The BFD neighborship fails with the EVPN VXLAN configuration after the Layer 2 learning restarts. PR1538600
- Configuration archival might not work. PR1540843
- The dcpfe process might crash in the specific MAC move cases and traffic loss might be observed in the EVPN-VXLAN scenario. PR1542709
- The JNH memory leak could be observed on MPCs or MICs. PR1542882
- Sessions creation rate is set to minimal rate after IDS and CPU throttling in place during DDoS attack. PR1544489
- The kmd process might crash when the interface flaps. PR1544800
- The VM host platform might get crashed continuously after performing upgrade or downgrade and booting up with the new image. PR1544875
- The high priority queue might consistently drop traffic after SIB goes offline. PR1545061
- Continuous rpd process errors might be seen and new routes fails to be programmed by the rpd process. PR1545463
- FPC might not boot-up on MX960 routers in certain condition. PR1545838
- The 40G or 100G interfaces might flap during unified ISSU if PTP is deactivated on the interfaces on MX platforms. PR1546704
- OSPFv3 session might keep flapping and OSPFv3 hellos might be dropped in the host path. PR1547032

- The PTP protocol might get stuck at initializing state on MX platforms. PR1547423
- WR Linux 6 platforms and WR Linux 9 platforms might be stuck after upgrading or downgrading image version and restarting the device. PR1547669
- Traffic for some IPv4 over IPv6 entries is dropped. PR1547681
- SR-TE might stay in the Up state when the routes are deleted through policy. PR1547933
- MX platforms might stuck after performing vmhost reboot post image upgrade. PR1548254
- The MS-MPC and MS-MIC located at VC-B might not work properly in an MX Series Virtual Chassis. PR1548340
- Traffic with jumbo frame might be discarded on the vMX platforms. PR1548422
- FPC crash might occur after flapping the multicast traffic. PR1548972
- When the MX Series device is in the SAEGW-U mode, in rare cases of a double back-to-back failover involving GRES and node association release, some access-peers might not be freed even after the sessions count associated with that peer reaches zero. PR1549689
- The firewalld process crash might be seen if deactivating/activating the firewall during back to back switchovers. PR1549856
- PKI CMPv2 client certificate enrollment does not work when using root-CA. PR1549954
- The LLDP adjacency might not be established for fxp interface. PR1550131
- Error messages are observed as the backup peer does not send marker acknowledgment for the last 360 seconds for vks 0 slave_ack=0 during ISSU. PR1550492
- Two Routing Engines might lose communication if they have different Junos OS versions on MX10003 platforms. PR1550594
- The adapted sample rate might get reset to the configured sample rate without changing the sampling rate information in sFlow datagrams after enabling sFlow technology on a new interface. PR1550603
- Deleting or deactivating the PS interface must not be allowed when use by BBE subscriber. PR1550915
- Unintended FPC restarts might be seen on MX10008 and MX10016 routers due to small timeout value between line card and chassisd process. PR1550917
- Certain MX platforms might reset and fail to boot due to a failure accessing Solid State Drive (SSD). PR1551047
- Silent compact flash (/dev/ada1) failure might occur during reboot or startup of router. PR1551171

- The softwire might not be established when connecting to a different AFTR. PR1552431
- Firmware versions for MPC11E line card were not getting displayed due to the changes made to the API in software required to read the firmware versions from the hardware. PR1552847
- The interface might not come up with 1G optics. PR1554098
- Unified ISSU upgrade from pre Junos OS Release 19.1 to Junos OS Release 19.1 and later might cause a few interfaces to go down. PR1554099
- The following error messages seen when we issue CLI commands to fetch host route scale: `Cattle-Prod Daemon received unknown trigger (type Semaphore, id 1)`. PR1554140
- `CoS WRED Curve: Create Expr Curve: No curve data points!!` error messages are seen when interpolate is configured under drop profile. PR1554220
- Global Ethernet flow-control should be disabled when PFC CNP is enabled on an interface. PR1554345
- The link on the Linux based LC is not brought down immediately after the FPC process(ukern/indus.elf) crashes or the process is killed. PR1554430
- On MX960 routers, SNMP index of output interface is reported as zero in the exported flow records of MPLS and MPLS-IPv4 sampling when `ipv4` tunnel-observation statement is deleted on the fly. PR1554489
- The subscriber sessions might be missed but stay in the authd after performing unified ISSU. PR1554539
- The device takes 3-10 mins to bring up the 100-1000 subscribers. PR1555216
- The chassisd process might crash with repeated configuration commits on MX204 and MX10003 routers. PR1555271
- The VGA might be down when configuring the IRB interface with multi VGA addresses. PR1555338
- The subscriber's RADIUS interim accounting statistics update might not work in some scenario. PR1555492
- Fabric self ping failure might be reported from MPC10 line card when MPC CPU is busy. PR1555802
- The following message is not generated on the MPC11E line card due to no power: `Chassisd SNMP trap Fru Offline`. PR1556090
- FPC with power related faults might get on-lined again once fabric healing has off-lined the FPC. PR1556558

- The dcpfe process might crash and restart with a dcpfe core file created while running the Type 5 EVPN VXLAN with 2000 VLANs. PR1556561
- On the MPC9E line card, core file is generated when SFB is online after ISSU of a GNF. PR1556627
- The framed route installed for a demux interface has no MAC address. PR1556980
- Script fails while committing the IPsec authentication configuration as the algorithm statement is missing. PR1557216
- The framed-routes are stuck in KRT queued (pending) add state when the `routing-service enable` is configured under dynamic-profile. PR1557230
- Multiple FPCs crash might be seen when performing GRES or FPC reboot repeatedly in subscriber scenario. PR1557294
- Packets corruption on 100G or 40G when interface is configured with protocol PTP. PR1557758
- The MAC addresses learned in a Virtual Chassis might fail aging out in MAC scaling environment. PR1558128
- Application identity unknown packet capture utility does not function when enhanced-services mode is enabled. PR1558812
- Rpd process generates core file after Routing Engine switchover. PR1558814
- 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 device might run out of service post GRES or unified ISSU. PR1558958
- MX Series with MPC10 and MPC11 line card might crash and restart when traffic is hitting a firewall filter having a term with syslog action configured. PR1559174
- On MX150 routers, the following continuous license error is observed: `[licinfra_set_usage_nextgen_async:1733] Invalid input parameters`. PR1559361
- The subscriber management infrastructure daemon (smid) process might be stuck at 100 percent. PR1559402
- Single rate three color policer does not work. PR1559665
- On MX960 routers, mismatch between YANG schema and RPC output are observed. PR1559810
- Zero suppression is disabled. PR1559882
- Untagged traffic routed over native-vlan might be dropped. PR1560038

- When the system has only one plane (in the process of plane offline or online), the MPC10-10C line card displays a destination error. PR1560053
- The PTP master line card servo might stuck in freerun state. PR1560074
- The jnxDomAlarmSet and jnxDomAlarmClear trap will be generated for a copper port. PR1560149
- The request system software validate command might corrupt installation of the junos-openconfig package. PR1560234
- The VXLAN queue DDoS violation and RARP packets flood might happen if receiving the RARP packets more than the supported DDoS bandwidth. PR1560243
- The PIC in SRX5K-SPC3/MX-SPC3 card might get stuck in offline status after flowd process crash occurs on it. PR1560305
- On MX240 routers, R0 overlay ping fails. PR1560408
- The class-of-service RED feature might work unexpectedly and cause traffic drop. PR1560495
- Telemetry might not work after reboot or upgrade. PR1560496
- Filters are not allowed on family any port-mirroring destination interface. PR1560624
- The FPC might reboot in a high-scale configuration scenario. PR1560757
- Interface does not able to send/receive packets after repeated link flaps on MPC10 and MPC11E line cards. PR1560772
- When LACP daemon is restarted, LACP local partner system id remains 0 in mc-ae output. PR1560820
- The native-vlan-id might not work as expected on MPC10E and MPC11E line cards. PR1560849
- FTP might fail when using in-band ports. PR1561146
- The tunable optics SFP+-10G-T-DWDM-ZR does not work. PR1561181
- SPC3 is not supported on MX in 21.1R1 for deployment. PR1561188
- The l2cpd process might generate core file on reboot. PR1561235
- The VIA headers might not be translated properly when the SIP ALG is enabled. PR1561312
- The `CdaExprClient: grpc api call ExprServerInfoGet failed` and `CdaExprClient: Failed to fetch server info error:5` are seen on all FPCs after restarting router or FPC restart. PR1561362
- Firewall filters might not work after unified ISSU. PR1561690

- Traffic drop might occur on all platforms running Junos OS when a GRE-based dynamic tunnel is configured. PR1561721
- Unable to open configuration database during USB upgrading. PR1561741
- After recovering from restart routing immediately, object-info anomalies is observed on rpd agent. PR1561812
- Continuous bbe-smgd core files are generated after restarting the smgd. PR1561855
- Interface loopback might not work if there is no optics connected to the port. PR1562471
- The dcpfe process might crash after deleting VXLAN configuration. PR1562692
- LICENSE_INVALID_FEATURE_ID syslog message is not being logged. PR1562700
- Commit issue is seen after loading limited-signed image through USB. PR1562723
- The rpd process might crash when the routing-instances are deleted and recreated quickly. PR1562905
- FPC Online/Offline through pinhole is not working. PR1563315
- The AppID DB not erased after the request system zeroize command. PR1563280
- Client authentication is failing after performing GRES. PR1563431
- Routing Engine switchover on-disk-failure does not work as expected when GRES is disabled. PR1563505
- Layer 2 interface information is not included in DHCPv4 option-82 circuit-id/remote-id DHCPv6 relay-agent-interface-id/relay-agent-remote-id options when service provider style configuration for switch interfaces is employed. PR1564010
- It might take a long time to create physical interfaces after restarting the FPC. PR1564156
- The following error message might be seen after unified ISSU: `Turbotx process not running`. PR1564418
- MX platforms with MX-SCBE3 might reboot continuously. PR1564539
- Old template is found in p2mp rsvp LSPs after adding new template. PR1564795
- Upon receipt of specific packets, BFD sessions might flap due to DDoS policer implementation in Packet Forwarding Engine. PR1564807
- Commit error observed when `tunnel-service` is configured on a PIC without explicit bandwidth. PR1565034

- On MX2010 and MX2020 routers, the following error message might be observed after switchover with GRES/NSR: `CHASSISD_IPC_FLUSH_ERROR`. PR1565223
- Unable to bring up more than one client on one VLAN at the same time. PR1565249
- PPPoE service-name-tables does not correctly count active sessions that matches agent-specifier ACI/ARI used for delay. PR1565258
- The KRT log file might continue to grow after removing the KRT log configuration. PR1565425
- Core files are seen at `grpc_slice_buffer_add_indexed` with LSR core profile configuration. PR1565427
- The mspmand crash might be seen on the PIC of MS-MPC and MS-MIC. PR1566325
- LLDP does not work on the management interface. PR1566454
- Pushing more than 2 MPLS labels on might not work. PR1566828
- Rpd core files are generated at boot time of a device. PR1567043
- The chassisd crash might be seen on MX platforms. PR1567479
- TLB composite next hop is installed incorrectly in other routing-instances. PR1567568
- Need to allow the tunnel interface as the peer-address for ALQ. PR1567735
- On MX204 routers, FPC might display high CPU utilization because of the JGCI background thread that runs for a long period. PR1567797
- State is not established for the `show bgp bmp station` *`name`* after the `authentication-key bmp-auth` is configured. PR1568046
- MAC addresses might not be installed in the EVPN MAC table due to route churn. PR1568130
- Memory might be exhausted when BGP sessions are unstable. PR1568551
- BFD flaps might be seen between leaf and core during spine reboot causing other protocols flap. PR1568615
- SPC3 card interfaces are not created. PR1568694
- IPv6 ping not working, when the strict uRPF is enabled. PR1568938
- Traffic might be dropped when the default route is changed in inet.0 table. PR1568944
- The `scu-class-name` statement is taking more than 60 seconds to come up with scaled aggregated Ethernet configuration. PR1568957
- The nsd process might crash after turning off the address translation for the NAT rules in the USF scenario. PR1568997

- The rpd process might crash while using BFD API to bring up the BFD sessions. PR1569040
- Traffic loss might be observed when SCU accounting is configured and `logical-systems` is enabled. PR1569047
- The agent sensor `__default_fabric_sensor__` are partly applied to some FPCs, which causes zero payload issue. PR1569167
- LLDP out-of-bounds read vulnerability in l2cpd. PR1569312
- Wi-Fi mPIM is reaching out to NTP and DNS servers. PR1569680
- The MPLS traffic passed through the back-to-back PE topology might match the incorrect CoS queue. PR1569715
- On MPC10 line cards, resolve to hold nh:776 not found in the database. PR1569829
- The mspmand process might crash if the packet flow-control issue occurs on MS-MPC and MS-MIC. PR1569894
- The log message `/tmp//mpci_info: No such file or directory :error[1]` might be seen on VM host platform. PR1570135
- The jinsightd process might be stuck with high CPU process utilization. PR1570526
- The bbe-smgd process might crash after committing several thousand addresses in a filter term. PR1570536
- The ZTP state machine might be stuck on the management interface for about 12 minutes. PR1570598
- Cleanup does not happen properly for subscribers stacked over static demux interface. PR1570739
- Upgrading with unified SSDs (2x32G SSD) might result in boot loop in certain scenario. PR1571275
- Packet loss might be observed when sample based action is used in firewall filter. PR1571399
- FPC crash might be seen when deleting a lot of multicast groups at the same time. PR1571890
- Switchover to backup Routing Engine if rpd was NSR ready and then crashed. PR1571914
- The gRPC session hanging in CLOSED state. PR1571999
- The grpcd process might crash and telemetry subscription will retry until grpcd restarts. PR1572107
- In transit spine devices, 100 percent DCI traffic loss is observed. PR1572238
- The TFEB/FPC might fail to be online after rebooting the system or the FPC if the `interface-set` is configured for CoS. PR1572348

- Segment routing might not work properly in IS-IS multiple levels setup. PR1572391
- The `show services mobile-edge sessions summary access-network-peers` command displays incorrect established subscriber output after the UPF handover ENB step. PR1572520
- On MX960 routers, the Require a Fan Tray upgrade alarm is raised when the top Fan Tray 0 is removed, even though the enhanced Fan Tray is already used. PR1572778
- A traffic loop might be observed after the VCP interface flap. PR1573047
- CFP unplugged message is not logged. PR1573209
- Fabric errors are observed and FPC processes might get offline when MPC3-NG or MPC3E line cards are installed along with MPC7/MPC10 and SCBE3/SCB4 operating in increased-bandwidth fabric mode. PR1573360
- The rpd process on the transit node might crash when MPLS traceroute on the ingress node is performed. PR1573517
- ARP traffic exceeding the policer limit is not discarded. PR1573956
- QSFP 4x10G interface might not come up after FPC reboot. PR1574279
- DS-Lite throughput degradation might be seen on MS-MPC. PR1574321
- Slow FPC heap memory leak might be triggered by flapping the subscribers terminated over multiple pseudowires. PR1574383
- The mpls-template for J-Flow version 9 cannot make a similar template to `mpls-ipv4-template` on MX MS-MIC/MPC. PR1574402
- PIM rib-group fails to be added in VRF. PR1574497
- On the EA-based cards IGMP group membership is displayed incorrectly. PR1575031
- PTP might be stuck in Phase acquiring state after ISSU upgrade PR1575055
- The rpd process might continuously crash if deleting forwarding-class policy with discard action. PR1575177
- The MPC10E line cards generates the following error message: `user.err aftd-trio: [Error] Em: root: Insert entry failed, entry:parentToken:747441 entryMask:ffffffffffffffff index:52`. PR1575310
- On the MX150 routers, the interface might take a long time to power down while rebooting, powering-off, halting, or upgrading. PR1575328
- The `show services service-sets statistics syslog` command returns the following error message as the service-set does not have the syslog configuration: `error: usp_ipc_client_recv_ 1237: ipc_pipe_read fails! error:No error: 0(0), tries:1`. PR1576044

- MPC crash might be seen when the `next-ip` action is used for filter-based forwarding. PR1576695
- The LLDP neighbor information displays hex string instead of chassis ID when subtype 1 is used. PR1576721
- The MS-MPC and SPC3 might reset on receiving the subscriber traffic. PR1576946
- Traffic drop and the aftd process crash are seen on MPC10 line card. PR1576997
- The following commit failure-error is observed: `Modified IFD "ae0" is in use by targeted BBE subscriber, commit denied - mtu config changed (1522), (1514)`. PR1577007
- Traffic loss might be seen when subscriber service over aggregated Ethernet bundle interface. PR1577289
- Object anomalies are seen with PTP TC configuration. PR1577375
- When line card is booted on Routing Engine 1 being master, Next-gen statistics failed to fetch the value of backup MAC address correctly. PR1577611
- Native sensors does not work for LDP LSP, LDP p2mp sensor. PR1577931
- The bbe-smgd process crash might be seen when the RADIUS server sends multiple CoA. PR1578162
- Mismatch in the snapshot recovery steps display message. PR1578556
- TACACS traffic might be dropped. PR1578579
- High FPC CPU usage might be seen when signal on the link is unstable. PR1579173
- Random or silent reboot might be seen. PR1579576
- On the MPC11E line card, system resource monitor does not list some of the available Packet Forwarding Engines. PR1579975
- On MX Virtual Chassis, data is missing in gRPC based components or sensor output. PR1580120
- Authentication might fail if the password contains special characters. PR1580003
- When analyzers mapped to channelized port, then the mirror might not happen properly. PR1580473
- BFD session with in-line mode might flap during network congestion. PR1580320
- The l2cpd process might crash on dual Routing Engines. PR1580479
- More than one subscriber on same VLAN fails to apply same FWF template. PR1580826
- Need to add support for Virtual Chassis licensing. PR1580880

- Issue is observed in telemetry when the set services analytics streaming-server configuration is present and server is not reachable. PR1581192
- Memory leak might happen due to stale NAT64 entries. PR1581231
- VM core messages are generated at 0xffffffff80443eef in kern_reboot. PR1581260
- The rpd process might crash on the new primary after performing graceful switchover. PR1581878
- Changing bandwidth statement does not take affect for SNMP ifHigSpeed oid until a PSX interface is disable/enabled. PR1582060
- The l2ald process generates the core file in `l2ald_vxlan_ifl_create_event_handler` while running the EVPN VXLAN scripts in VQFX during the PCT submission. PR1582128
- Communication between two CE devices might be failed when BGP rib-sharding is enabled. PR1582210
- Pciephy and firmware download are not working after migration to 6.5.19. PR1582244
- The bbe-smgd process on both routing engines might crash due to a rare timing issue after log out of subscribers over pseudowire. PR1582356
- On MX960 devices, the 400G and 4x100G optics laser restores after reboot despite interface disable being configured. PR1582418
- Destination port might be incorrectly set on MS-MPC and MS-MIC in a DS-Lite scenario. PR1582595
- Node locked license addition fails. PR1582704
- Configuring or removing the `hierarchical-scheduler` or `per-unit-scheduler` might cause traffic to stop forwarding. PR1582724
- The firewall filter logs are incorrectly populated the protocol entries. PR1582780
- Reset JBS, JAS, JPS definition to align with Hawk License model. PR1583438
- Reset PFL, AFL definition to align with Hawk License model. PR1583439
- SNMP SysObjectID.0 is empty with enabled unified-services. PR1583534
- TCP connection to syslog server might fail to be established after adding tcp-log configuration for an existing service set. PR1583979
- The jsd process hogging CPU. PR1584357
- Traffic might not get filtered properly when security-intelligence profile is configured on the MX platforms. PR1584377

- The rpd process might crash due to a rare timing issue if both BGP Local-RIB and Adjacency-RIB-In route monitoring are enabled in BMP. PR1584560
- Bridge domain names information is not displayed properly in the `show bridge statistics instance` command. PR1584874
- After changing configuration, the `show bridge statistics` command displays extreme larger value. PR1584876
- Traffic impact might be seen when tunnel-services bandwidth is configured. PR1584969
- GRE OAM packets are sent through queue 0 with force-control-packets-on-transit-path statement enabled. PR1586169
- Traffic drop after enabling flexible-queuing-mode on MPC2E line cards. PR1586403
- The l2ald process might crash on changing the routing-instance. PR1586516
- Inter and intra VNI traffic drop might occur in spine with EVPN-VXLAN CRB configuration. PR1586537
- The rpd process generates core file if the show igmp continuous stats command is executed after GRES. PR1587023
- Mspmand.core.ms32.0.gz is found while testing memory-usage prints garbage value. PR1587103
- The SNMP trap for MAC notifications might not be generated when an interface is added explicitly under switch-options. PR1587610
- The bbe-smgd might crash if the staled ACI based subscribers are not cleaned up properly. PR1587792
- The na-grpc process crash might be seen and existing telemetry connections will be disconnected. PR1587956
- The rpd process crash might be observed on the router running in a scaled setup. PR1588439
- The bbe-statsd memory leak might be observed on backup Routing Engine during subscriber's login and logout. PR1589081
- The jsd process crash might be seen in a rare condition in a telemetry scenario. PR1589103
- The l2cpd process might crash. PR1589216
- Allow default license for FBF, CFM, VRRP, Q-IN-Q, MC_LAG, TIMING, IGMP, PIM, GRE_TUNNEL, RIP, OSPF, Virtual Chassis, and sFlow. PR1589920
- Expected snooping route is not observed after configuring one bridge with snooping and add interface check. PR1590278

- Some times `show chassis fabric reachability extended detail` command shows that fabric healing is complete for Phase 2, while the links to few FPCs or SLCs are still under training. PR1590335
- Traffic loss might be observed due to FPC crash in a scaled subscriber scenario. PR1590374
- If the CoS CR-features used by VBF service is configured, MPC might crash with subscriber PR1591533
- The clear-ipsec-sas-for-duplicate-ts is not clearing secuar Access (SA) for duplicate traffic selectors (TS). PR1591735
- The xSTP might not get configured when it is enabled on a interface with SP style configuration on all platforms. PR1592264
- Routing Engine kernel might crash due to logical interfaces of aggregated interface adding failure in Junos OS kernel. PR1592456
- Any mmcq based services might crash due to shared memory queue issue happens in a rare condition. PR1592889
- The TCP keepalive message might not be processed by the private network host. PR1593226
- Fabric errors will be generated after swapping MPC10E with MPC7E line card in the same slot. PR1593821
- On MX5, MX40, and MX80 routers, TEB stuck in present state. PR1595107
- On MX Series platforms with EVPN-VXLAN with `shared-tunnel` configuration, when there is BGP flap or restart of l2ald, then info logs appear. PR1595203
- The l2ald process might crash on all leaves and spines after a new leaf is added to the EVPN fabric. PR1596229
- Traffic loss might happen periodically in MACsec used setup if Routing Engine is working under a pressure situation. PR1596755
- Major alarms on all FPCs in chassis after some time from boot up. PR1597066

Class of Service (CoS)

- The explicit classifier or rewrite-rule might not work as expected for a logical interface if the wildcard configuration is also applied. PR1556103
- On the MPC7E line card, the BPS counter of the egress queue displays incorrect BPS value when the cell mode is configured on the static interface. PR1568192
- FPC crash might be observed after the show class-of-service command execution. PR1568661

- Class of service commands will be auto sorted and will not be ordered as per the user configuration. PR1568907
- Unable to configure policer with bandwidth-limit greater than 50g. PR1575049

EVPN

- Rpd memory leak might occur when the EVPN configuration is changed. PR1540788
- The rpd process might crash after adding `route-target` on a dual Routing Engine system under the EVPN multihoming scenario. PR1546992
- The rpd process might crash under EVPN-VPWS environment. PR1562160
- Prefix added to the mhevpn.evpn.0 output route table triggers TC failure. PR1566429
- Traffic might drop on multicast based VXLAN tunnel. PR1567209
- Policy with mac-filter-list might not work if the change is not related to that policy committed in an EVPN scenario. PR1567623
- ESI preference is not preferred when configured on lo0 for multicast VXLAN. PR1570618
- The multicast traffic loss might be seen in EVPN VXLAN scenario with CRB multicast snooping PR1570883
- The mustd process generates core file during upgrading or while committing a configuration. PR1577548
- Rpd process might crash in high scaled EVPN VXLAN scenario. PR1581674
- Multicast traffic loss might be seen in EVPN setup with IGMP snooping used. PR1582134
- After the device reboot in an EVPN-VXLAN setup with graceful restart, EVPN routes are not advertised to EVPN peers until rpd is up for 180 seconds. PR1586246
- The BUM traffic might lose after triggering GRES+NSR in an EVPN-MPLS or EVPN-ETREE scenario. PR1586402
- The traffic might be dropped when EVPN and L3VPN routes are resolved using the same MPLS-over-UDP tunnel. PR1587204
- The traffic might be dropped in an EVPN-VXLAN multihomed scenario. PR1590128

Forwarding and Sampling

- After routing restarts, the remote mask that the routing daemon sends might be different from the existing remote mask that the Layer 2 learning daemon had before restart. PR1452990
- User-defined ARP policer is not applied on aggregated Ethernet interface until firewall process is restarted. PR1528403
- The dfwd process might crash when implementing non-contiguous firewall filter. PR1555724
- The configuration archive transfer-on-commit fails. PR1563641
- In the VXLAN scenario, the locally originated packets have UDP source port 0. PR1571970
- The pfed memory leak might be observed. PR1573285
- The l2ald process might crash on changing the routing-instance. PR1584737

General Routing

- The ndp process might reach to 100 percent and might result in traffic drop. PR1551644
- More memory usage might occur in ndpd (NDP daemon). PR1568370
- Silent switchover might be triggered on executing restart routing. PR1570993
- The DHCP ALQ is not working as expected. PR1578543
- Rpd process core file might be seen on the backup Routing Engine after a switchover with graceful restart is enabled. PR1582095
- After performing NSSU, `timeout waiting for response from fpc0` error message is seen while checking version detail. PR1584457

Infrastructure

- On Virtual Chassis and Virtual Chassis fabric, HEAP malloc(0) detected. PR1546036
- When device trying reboot from OAM might get stuck in OK prompt and leading to reboot from Junos OS. PR1555748
- Some MAC addresses might not be aged out. PR1579293

Interfaces and Chassis

- Backup Routing Engine or backup node might get stuck in bad status with improper backup-router configuration. PR1530935
- On the MPC10 line card, DMRs or SLRs are not received with an EVPN up MEP on the aggregated Ethernet interface with normalization. PR1543641
- An lacpd core file is obserevd after router reboot. PR1553196
- Block duplicate IP across different logical interfaces inside same routing instance. PR1555861
- Sessions are flapped after applying the action profile on the router. PR1561044
- The input errors counter command on the monitor interface command does not work. PR1561065
- The ppmd process might crash when VRRP is configured. PR1561281
- MAC address entry issue might be observed after the MC-LAG interface failover. PR1562535
- Traffic loss might be seen while verifying VRRP state machine functionality. PR1564551
- Unable to set `member-id` as Routing Engine is in synching mode forever when its having invalid Virtual Chassis data. PR1569556
- The `show interface interface name | display xml` command output displays the media type if-media-type also along with other parameters. PR1574035
- There might be increase in memory for the fabspoked process. PR1574391
- MX Virtual Chassis ISSU incompatible FRU offline can result in unexpected FPC restarts after ISSU completes. PR1575687
- The following errors are generated during GRES: `VRRPMAN_PATRICIA_GROUP_ADD_FAIL: vrrp_ifcm_send_bulk: Failed to add group to patricia tree key and VRRPMAN_ENTRY_KEY_PRESENT: vrrp_ifcm_send_bulk: Already an entry present with the key`. PR1575689
- MC-AE interfaces might go down if same VRRP group-id is configured on multiple IRB units. PR1575779
- The `show interface description` display order is different. PR1576224
- Newly added MC-LAGs do not come up after Routing Engine switchover. PR1583547
- NCP/PPP negotiation Max-Failure retry count are not configurable. PR1584168
- Unable to configure pseudowire interface on an MX10003 in Virtual Chassis mode. PR1587499
- The VRRP host cannot be reached if `native-vlan-id` is configured. PR1595896

Intrusion Detection and Prevention (IDP)

- Adding signature in packet drop reason and sending to record packet drops module. PR1574603

J-Web

- J-Web allows a locally authenticated attacker to escalate their privileges to root. PR1511853
- To improve performance in Monitoring > Network > Interfaces page, Admin Status is removed, Services and Protocols data merged into one Host inbound traffic. PR1574895

Juniper Extension Toolkit (JET)

- TCP connection might not be established while creating the default gRPC channel with fw_channel name. PR1559064
- The custom JET APP will be lost after rebooting. PR1570563

Junos XML API and Scripting

- Multiple vulnerabilities in cURL resolved. PR1562153

Layer 2 Features

- LACP gets into detached state when deleting VLAN on aggregate interface configured on SP style. PR1555862
- Traffic forwarding for VLAN 2 might not be correct when a VLAN member is removed from the ESI interface. PR1570446
- LACP does not come up in non-oversubscribed mode for a set of ports. PR1563171
- The `clear vpls mac-address` could result in rpd core. PR1573406

Layer 2 Ethernet Services

- The copying of files to the RCB over WAN ports is slow. PR1496895
- Aggregated Ethernet interface flap might be seen during NSSU. PR1551925
- DHCP packet drop might be seen when the DHCP relay is configured on a leaf device. PR1554992
- In a DHCP relay configuration with active lease query, some subscriber's active on master might get logged out. PR1559269

- Receipt of malformed DHCPv6 packets causes jdhcpd process to crash and restart. PR1564434
- DHCPv6 option 18 and option 37 might not be created in a DHCP dual stack scenario. PR1564778
- The jnxJdhcpLocalServerMacAddress (.1.3.6.1.4.1.2636.3.61.61.1.4.3) returns incorrect format of the MAC address. PR1565540
- The Option 82 information is incorrectly cleared by the DHCP relay agent. PR1568344
- The DHCP client will be offline for 120 seconds after sending the DHCPINFORM message in a the DHCP relay scenario. PR1575740
- DHCP relay drops packets during the renewal DHCP process. PR1576417
- The jdhcpd might crash if the relay-source lo0 is enabled in the DHCP relay. PR1580724
- The jdhcpd process might not respond to any discover message when it is in `clients waiting to be restored` state. PR1592552

MPLS

- The rpd process might crash in a corouted bidirectional RSVP LSP scenario. PR1544890
- A new LSP might not be up even if bypass LSP is up and setup-protection is configured. PR1555774
- Incorrect EXP bit change might be seen in certain conditions under MPLS scenario. PR1555797
- MPLS-LIB memory leak might be seen in segment routing scenario. PR1556495
- Traffic loss might be observed during rpd crash when RSVP signaled P2MP LSP is configured. PR1559022
- LDP routes might be stuck when BGP LU session is down. PR1562884
- Traffic sent over an LSP might be dropped if two consecutive PLRs along the LSP perform local repair and bypass protecting the second PLR fails. PR1566101
- Unexpected LSP packet count is found in the ingress MPLS LSP statistics. PR1570382
- The rpd process generates core file when deactivating PCEP protocol followed by RSVP protocol. PR1579370
- The suboptimal routing issues might be seen in case LDP route with multiple next hops. PR1582037
- Add `lsp-ping-multiplier` option support for LDP-OAM similar to RSVP-OAM. PR1582254
- MBB is not triggered when LSP is reverting back to primary path. PR1587704

Multicast

- FPC might crash in a multicast scenario. PR1569957

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 mib2d process crashes and generates a core file on backup Routing Engine. PR1557384
- Context registration from l2cpd to snmpd might fail after l2cpd service restart. PR1561736
- SSH connection might become unresponsive and logs the following message: `kern.maxfiles limit exceeded by uid`. PR1567634
- Slow memory leak might be observed for snmpd process. PR1575790

Platform and Infrastructure

- Traffic loss might be observed due to FPC crash on MX platfoms. PR1482683
- Interwork failure as RPM client and TVP platforms as RPM server (and vice versa). PR1508127
- Console access on backup Virtual Chassis member is not allowed. PR1530106
- The npc process generates the core file in `igmp_process_wakeup_events,igmp_pfe_thread,thread_detach_tty`. PR1534542
- Packets transiting via multicast-based VXLAN VTEP interface might be dropped post FPC restart. PR1536364
- The queue-counters-srx-reserved-buffer-bytes count is 625000 bytes, expected buffer is 2500000. PR1538286
- The following major error message might cause the Packet Forwarding Engine to disable: `XQ_CMERROR_SCHED_L3_PERR_ERR`. PR1538960
- Subscribers over an interface-set might not be able to login. PR1539260
- The kernel might crash if GRES is performed on either new iteration or after swapping the Routing Engine and restoring the HA configuration. PR1549656

- Traffic loss might be seen as logical interface policer is not processed properly during filter migration. PR1551394
- Traffic is not forwarded over IRB to a Layer 2 circuit on the lt interfaces. PR1554908
- SPC3 might not come up after the system reboot. PR1555904
- The IPv4 EXP rewrite might not work properly when `inet6-vpn` is enabled. PR1559018
- The BUM frame might be duplicated on an aggregate device if the extended-port on the satellite device is an aggregated Ethernet interface. PR1560788
- Interfaces statistics not updated on aggregated Ethernet interface as expected with CCCOAE configurations. PR1561304
- Multicast traffic with incorrect source MAC address might be observed from IRB interface. PR1561313
- The DHCPv4 request packets might be incorrectly dropped when DDoS attack occurs. PR1562474
- Traffic loss might be observed due to FPC crash on MX platforms. PR1563144
- The mtr process might hog CPU when the traceroute monitor command is paused. PR1563298
- The `enforce-strict-scale-limit-license` configuration enforces subscriber license incorrectly in the ESSM subscriber scenario. PR1563975
- The `Last flapped` timestamp for interface fxp0 gets reset every time the `monitor traffic interface fxp0` command is executed. PR1564323
- PFEX might crash when soft error recovery feature is enabled on Packet Forwarding Engine. PR1567515
- Reclassify the severity of the CMERROR `XMCHIP_CMERROR_DDRIF_PROTECT_WR_RD_SRAM_RUNN_CHKSM` from major to minor. PR1568072
- The following error message is observed: `toe_lu_stats_ucode core found @ jbeta_fcv_alloc_fcv_idx_global jbeta_sfilter_fcv_cb bwy_dfw_sfilter_fcv_cb`. PR1569328
- The following error message is observed: `pfe err-jnh_physmem_add_resvd_to_cntr(18014): PFE 0 jnh_app 0x08020860, add ox00080000 from 0x00b00000-0x00b80000 to baMask 0x1`. PR1570631
- FPCs might crash randomly while deleting the interface-set in the system. PR1571192
- When EVPN-VXLAN is configured, the next-hop memory leak in MX Series ASIC happens whenever there is a route churn for remote MAC-IP entries learned bound to the IRB interface in EVPN-VXLAN routing instance. When the ASIC's next-hop memory partition exhausted the FPC might reboot. PR1571439

- Scale-subscriber license might not be updated properly on the backup Routing Engine which leads to `License grace period for feature scale-subscriber(44) is about to expire` alarm after GRES. PR1573289
- The following error message is observed: `cassxr_err_addr(8593): Uninitialized Read Error @ EDMEM[0x7cb601b0]`. PR1573920
- Introduce two new major CMERRORs for XM chip-based line card to stabilize the running device. PR1574631
- Memory partitioning issue might happen on Packet Forwarding Engine after applying sampling and the flex-flow-sizing to the MX Series with MPCs/MICs based line-cards. PR1575994
- If committing the source-address addr routing-instance and then delete the source-address addr in private edit mode, commit fails with a warning message. PR1582529
- VRRP device originally taking backup role might cause destination IP unreachable after VRRP mastership switch-over. PR1584115
- FPC crash might be observed in a scaled firewall configuration on MX Series platforms. PR1586817
- The traffic might not failover with `shared-bandwidth-policer` enabled on aggregated Ethernet. PR1588708

Routing Policy and Firewall Filters

- Global variable policy_db_type is not set to the correct value on failure. PR1561931
- Generated route goes to the hidden state when the `protect core` command is enabled. PR1562867
- The rpd process might crash when the deletion of routing table occurs. PR1565629
- The rpd might crash due to the source-address-filter-list enabled within the policy. PR1565891
- Traffic loss might be observed during rpd process crash when `auto-bandwidth` is configured. PR1579830
- The bbe-smgd process fails when reading configuration for address mask prefix-length when configured in a policy statement, causing the service profile to fail. PR1583535

Routing Protocols

- The rpd process crashes when a fresh router is configured with IS-IS and RIB-group to leak inet3 routes from no-forwarding to primary instance in single commit. PR1534486
- Unexpected packet loss might happen due to inet-vpn routes not valid in vrf.inet.0 and bgp.l3vpn.0 routing tables. PR1543717
- Convergence time is high when the IGMP snooping configuration is deleted. PR1550523

- Specific packets can trigger rpd crash when BGP origin validation is configured with RPKI. PR1556207
- Route validation states might flip between VALID, INVALID, and UNKNOWN in some corner case. PR1556656
- Multipath information is displayed for BGP route even after disabling the interface for one path. PR1557604
- BGP-LU session flap might be seen when the AIGP is used. PR1558102
- The ISO routes are not leaked in default (master) instance after switchover or reconfiguration. PR1558532
- Traffic loss might occur for stitched traffic from segment routing towards LDP if no-eligible-backup is configured. PR1558565
- When admin-color based policy evaluation happens with the policy LFA configuration, the backup next hop chosen (among the possible different backup next hops) might not be correct. PR1558581
- Incorrect Active, Received, or Accepted counters in the `show bgp summary` command. PR1558678
- The rpd process might crash when applying the BGP route policy change. PR1560037
- VPN routes learned from core were not advertised to the CE devices when BGP sharding is configured. PR1560661
- All the Layer 3 VPN route resets when a VRF is added or removed. PR1560827
- Duplicate LSP next hop is shown on inet.0, inet.3 and mpls.0 route table when `ospf traffic-engineering shortcuts` and `mpls bgp-igp-both-ribs` are enabled. PR1561207
- Incorrect SPF calculation might be observed for OSPF with `ldp-synchronization hold-time` configured after the interface flap. PR1561414
- The ppmd memory leak might cause traffic loss. PR1561850
- The rpd process might crash with dynamic tunnels configured. PR1562458
- The rpd process might crash on the backup Routing Engine after rpd process restart is triggered on the primary Routing Engine. PR1563350
- The rpd process might crash if there are more routes changed during the commit-sync processing window. PR1565814
- There might be traffic loss when GRE interface flaps. PR1566428
- The rpd process might crash in BGP L2VPN scenario due to memory corruption. PR1567026

- The rpd process might crash when the BGP session re-establishes or flaps. PR1567182
- The rpd memory leak might be observed during CLI or ephemeral commits in a OSPFv2 scenario. PR1568157
- Traffic loss might be observed due to the rpd process crash in BGP multipath scenario. PR1568600
- The rpd process might crash continuously when MoFRR is configured along with TI-LFA. PR1568750
- Traffic might be lost during mirror data transmit from the primary ppmd or bfdd. PR1570228
- There might be 10 seconds delay to upload the LSP on the point-to-point interface if rpd process is restarted on its direct neighbor. PR1571395
- SNMP MIB ospfv3NbrState is returning drifted value. PR1571473
- Incorrect authentication-algorithm is set in BGP neighbor. PR1571705
- Rpdagent core seen while testing BFD state replication. PR1571824
- After first parallel ISSU, subsequent ISSU aborts with `Aborting Daemon Prepare` due to BFD abort state. PR1572265
- The DHCP BFD subscriber session does not come up on the MPC Type 2 card and gets stuck in the `Down` state. PR1572577
- The DHCP packets might be dropped in the Static VXLAN scenario. PR1576168
- Provide a CLI option to change default BGP listen port. PR1576728
- The ppmd might crash when enabling MD5 authentication on OSPF with BFD flapping. PR1576893
- BGP session flap might be observed after the Routing Engine switchovers when the VRRP virtual address is used as the local address for the BGP session. PR1576959
- Multicast traffic loss might be observed due to logical PIM de-encapsulation interface is not created as expected. PR1577461
- The rpd process might crash when two or more routing instances are deleted in one shot. PR1578740
- The dcpfe process might crash when any interface flaps. PR1579736
- Rpd core found at `thread_next_node jnx_bgp_tunnel_encaps_attr_tunnel_count jnx_bgp_tunnel_encaps_attr_set_tunnel`. PR1579818
- BGP replication might be stuck in rare and timing conditions. PR1581578
- BGP session carrying VPNv4 prefix with IPv6 next hop might be dropped. PR1580578

- The rpd process might crash in BGP and MPLS scenarios. PR1581794
- The route resolution issue is observed after controller facing Packet Forwarding Engine restart or core interface disable or enable PR1581845
- Possible rpd process might crash with the `routing-options transport-class` configuration during the restart. PR1582081
- The voice VLAN might not get assigned to the access interface. PR1582115
- With IGMP snooping implemented, there is unexpected jitter issue that could cause traffic loss. PR1583207
- SSH cipher option Triple-DES is disabled in FIPS mode. PR1583470
- The rpd process crash might be seen in certain IS-IS scenario. PR1583484
- On rare occasion, rpd process core might be observed on backup Routing Engine after loading a new image. PR1583630
- Origin-validation replication status shows up in the `show task replication` command output even when it is not configured. PR1583692
- The rpd process might crash when BGP RPKI session `record-lifetime` is configured less than the hold-time. PR1585321
- The rpd process might crash after committing with the configured static group. PR1586631
- Incorrect BGP next-hop advertisement in a L3VPN scenario. PR1587879
- The multicast traffic loss might be observed after unified ISSU is performed. PR1588555
- The rpd process might crash in a scaled routing instances scenario. PR1590638
- when you disable or enable BGP in a short time interval on a scaled NSR router can result in backup rpd process restart. PR1591717
- The remote LFA backup path might not be formed. PR1592424
- BGP egress-TE routes lose to BGP routes using the same protocol preference. PR1593332
- The routing process might crash due to memory corruption while processing BGP multipath route. PR1594626

Services Applications

- The CoA with LI-on or LI-off message might be dropped during CoA process. PR1554618

- Memory leak might be observed in a tunnel flapping scenario. PR1567291
- Support to clear l2tp session based on routing-instance name filter. PR1580984
- IWF AVP value might not be reflected properly on LTS. PR1581096

Subscriber Access Management

- BBE-SMGD configures incorrect `vbf_accurate_accounting_bits` to the Packet Forwarding Engine. PR1515899
- The authd might crash after performing unified ISSU in a MX BNG scenario. PR1570096
- CoA request might not be processed correctly from time to time. PR1571501

User Interface and Configuration

- The `port_speed` configuration details not present in the picd configuration for ports et-0/0/128 and et-0/0/129. PR1510486
- The configuration under groups stanza is not inherited properly. PR1529989
- Commit might fail after the Routing Engine switchovers. PR1531415
- The operational state would be incorrect on the system and CoS schedulers configuration change might not take effect. PR1536615
- The mgd process might crash when performing rollback command. PR1554696
- The chassisd core files might be observed if PIC number 2 or 3 is used on MX204 platforms. PR1555685
- If the xml output from the `request vmhost mode test | display xml rpc` command is picked and used in NETCONF fails. PR1559786
- Memory leak on eventd might be seen when running the request system script event-scripts reload command. PR1570580
- The LACP might stop working after disabling LACP sync-reset. PR1576146

Virtual Chassis

- Virtual Chassis might not come up after upgrade when QSFP+-40G-SR4, QSFP+-40G-LR4, or QSFP +40GE-LX4 is used. PR1579430

VPNs

- Traffic from the reverse direction might cause traffic loss for up to 1 second with NSR switchover. PR1558395
- Type7 messages might not be sent from egress PE device resulting in Type 3 or Type 5 messages not created for some S, Gs in source PE devices. PR1567584
- The rpd might crash during a race condition under BGP multipath scenario. PR1567918
- The iked process might crash when IKEv2 negotiation fails on MX devices. PR1577484
- The rpd process might crash in the NG-MVPN scenario. PR1579963
- The traffic of the draft-rosen multicast VPN might lose after switching over the Routing Engines. PR1584720

Documentation Updates

There are no errata or changes in Junos OS Release 21.2R2 documentation for the MX Series routers.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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
MX5, MX10, MX40,MX80, MX104	YES	NO
MX240, MX480, MX960, MX2010, MX2020	NO	YES

Basic Procedure for Upgrading to Release 21.2R1

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-x86-32-20.4R1.9-signed.tgz
     ```

   - For 64-bit Routing Engine version:

     ```
     user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-20.4R1.9-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-x86-32-20.4R1.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-20.4R1.9-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 21.2R1, 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.]

NOTE: After you install a Junos OS Release 21.2R1 jinstall package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add no-validate` command and specify the jinstall package that corresponds to the previously installed software.

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

Procedure to Upgrade to FreeBSD 6.x-Based Junos OS

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

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

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

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

2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the Release drop-down list to the right of the Download Software page.
4. Select the Software tab.
5. In the Install Package section of the Software tab, select the software package for the release.

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

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

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

```
user@host> request system software add validate reboot source/jinstall-ppc-20.4R1.9-signed.tgz
```

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

```
user@host> request system software add validate reboot source/jinstall-ppc-20.4R1.9-limited-signed.tgz
```

Replace source with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 21.2R1 jinstall package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the jinstall package that corresponds to the previously installed software.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19,4, 20.2, and 20.4 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 21.2R1

To downgrade from Release 21.2R1 to another supported release, follow the procedure for upgrading, but replace the 21.2R1 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

These release notes accompany Junos OS Release 21.2R1 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

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

What's New in 21.2R1

IN THIS SECTION

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

Application Identification (AppID)

- **Application-based multipath routing (AMR) improvements (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, SRX550 HM, and vSRX)**—Starting in Junos OS release 21.2R1, we've introduced the following improvements for AMR:
  - Support for the traffic in reverse direction
  - Queuing mechanism for out-of-order packets at the receiving device

- Association of AMR rules and service-level agreement (SLA) rules with advanced policy-based routing (APBR) rule in an APBR profile
- Link selection option that includes overlay interfaces such as GRE and secure tunnel
- Enablement of AMR in one of the two modes—SLA violation mode or standalone mode
- Support for IPv6 traffic
- Support for AMR over IPsec and GRE sessions

[See Application-Based Multipath Routing.]

- **Multicast support in SD-WAN deployments (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX4100, SRX4200, SRX4600, vSRX)**—Starting in Junos OS Release 21.2R1, we've added support for multicast traffic on SRX Series devices in Provider Edge (PE) for SD-WAN deployments. The support for multicast traffic is available when the security device is operating with forwarding option set as flow-based.

  Support for multicast traffic results in bandwidth preservation and more efficient traffic flows.

  See [mode (Security Forwarding Options) and Virtual Routing and Forwarding Instances in SD-WAN Deployments].

- **SLA link preference enhancement (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, SLA link preference for security device interfaces supports custom link tags. You can define the link preferences using the `preferred-tag` and `affinity` options.

  This enhancement allows application traffic to switch from a lower-priority link to a higher-priority link that meets SLA requirements.

  [See Understanding Link-Type Affinity for the Preferred Link and sla-rule.]

- **Application-based load balancing support for APBR (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, security devices support application-based load balancing for advanced policy-based routing (APBR). The APBR achieves load balancing by moving the application traffic in multiple WAN links using user-defined link selection criteria. The link selection criteria for application traffic depends on the link tag and link priority preference settings you defined for the advanced policy-based routing (APBR) interface. The application traffic distribution through the selected links depends on the link weight configuration.

  This feature improves the application traffic distribution performance for APBR and application quality of experience (AppQoE).

  [See Advanced Policy-Based Routing, sla-options, and interface.]

Authentication and Access Control

- **Display dynamic-applications and URL category hit counts in a security policy (NFX Series and SRX Series)**—Starting in Junos OS Release 21.2R1, we've enhanced the `show security policies hit-count` command to include the dynamic applications and URL categories options. You can now display the utility rate of the policy according to the number of hits for the dynamic applications and URL categories.

  [See show security policies hit-count.]

Flow-Based and Packet-Based Processing

- **GRE acceleration enhancement (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.2R1, security devices support the existing PMI and GRE acceleration for non software-defined WAN (SD-WAN) deployments.

  PMI and GRE acceleration improve GRE and MPLS-over-GRE performance.

  [See gre-performance-acceleration and show security flow status.]

- **Multicast support in SD-WAN deployments (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, we've added support for multicast traffic on security devices in Provider Edge (PE) for SD-WAN deployments. The support for multicast traffic is available when the security device is operating with forwarding option set as flow-based.

  Support for multicast traffic results in bandwidth preservation and more efficient traffic flows.

  [See mode (Security Forwarding Options) and Virtual Routing and Forwarding Instances in SD-WAN Deployments.]

What's Changed

IN THIS SECTION

Learn about what changed in Junos OS main and maintenance releases for NFX Series devices.

What's Changed in Release 21.2R1

There are no changes in the behavior of Junos OS features or in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for NFX Series devices.

Known Limitations

There are no changes in behavior or syntax in Junos OS Release 21.2R1 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

Learn about open issues 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.

Interfaces

- When you run a `show interface` command on NFX150 devices to check the interface details, the system does not check whether the interface name provided is valid or invalid. The system does not generate an error message if the interface name is invalid. PR1306191

Virtual Network Functions (VNFs)

- On NFX150 devices, before reusing a VF to Layer 3 data plane interfaces (for example, ge-1/0/3), which was earlier allocated to a VNF, you must restart the system. PR1512331
- On NFX Series devices, while configuring `vmhost vlans` using `vlan-id-list`, the system allows duplicate VLAN IDs in the VLAN ID list. PR1438907

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 21.2R1

IN THIS SECTION

Interfaces

- On NFX250 devices, a VNF interface is not brought down when the VNF interface is mapped to an already link down or disabled peer physical interface. PR1555193

Performance Modes

- You cannot enable the trust mode on an SR-IOV virtual function assigned to a VNF. PR1593037
- A message is provided in syslog if reboot is required for the mode modification to take effect in custom mode. PR1555465

Platform and Infrastructure

- RPD core file is generated when the device reboots and daemon restarts. Daemon recovers and there is no service impact on routing protocol usage. PR1567043
- On NFX350 devices and the SRX5000 line of devices with SPC3 card, the DPD Gateway failover feature is not supported. PR1564715
- The l2cpd core files might be seen on reboot. PR1561235
- On NFX150 devices, when J-Flow v5 is configured and the J-Flow v5 server is reachable through an IPsec tunnel, and the MTU size of this IPsec tunnel is configured as 1500, the J-Flow packets are not generated on NFX Series devices. As a workaround, use J-Flow v9 or IPFIX version, instead of J-Flow v5, to enable the J-Flow functionality on NFX Series devices. PR1539964
- You can transfer file from USB to hypervisor by enabling the usb-pass-through functionality. PR1535220
- On NFX150, NFX250 NextGen, and NFX350 devices, the `EmulatorPin CPUSet` option does not get configured, which might result in vCPU running on a higher level up to 100%. PR1540564
- The DSL SFP firmware cannot finish upgrade successfully through vmhost reboot. PR1547540

Documentation Updates

There are no errata or changes in Junos OS Release 21.2R1 documentation for the NFX Series documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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 21.2

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 21.2R1:

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

These release notes accompany Junos OS Release 21.2R1 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

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

What's New in 21.2R1

IN THIS SECTION

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

Hardware

- The following methods to protect the chassis from excessive current draw and temperature conditions are supported:
  - Configure Junos OS to automatically shut down the PSM, or raise an alarm and log the event when a field-effect transistor (FET) failure is detected in the power supply module (PSM) by using the specified command. [See thermal-health-check].
  - Configure upgrade of the PSM firmware that will take actionwhen there is an FET failure by using the specified command. [See request system firmware upgrade].
  - Configure Junos OS to raise an alarm and log events when a PSM with upgraded firmware version shuts down due to an FET failure, Junos OS on the attached device.
  - Configure a monitor to check how much power the chassis draws from the PSM using the specified command. If the system draws more power from the PSM than what it should consume, Junos OS raises an alarm or shuts down the system. [See watchdog (PSM)].
    [See Handling Thermal Health Events Using Thermal Health Check and PSM Watchdog].

- **Support for AOC transceivers (PTX1000)**—Starting in Junos OS Release 21.2R1, the PTX1000 routers support the following active optical cable (AOC) transceivers:
  - JNP-40G-AOC-1M
  - JNP-40G-AOC-3M
  - JNP-40G-AOC-5M
  - JNP-40G-AOC-7M
  - JNP-40G-AOC-10M
  - JNP-40G-AOC-15M
  - JNP-40G-AOC-20M
  - JNP-40G-AOC-30M

  [See Hardware Compatibility Tool.]

High Availability

- **NSR support for RSVP-TE dynamic tunnels (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support nonstop active routing (NSR) for RSVP-Traffic Engineering (RSVP-TE) dynamic tunnels.

  [See Nonstop Active Routing Concepts.]

- **NSR support for SR-TE (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support NSR for segment routing–traffic engineering (SR-TE), allowing for hitless traffic flow on Routing Engine switchover. Routes using next hops from SR-TE policies that don't support NSR might experience traffic loss on switchover. The SR-TE policies that don't support NSR are DCSPF and Path Computation Element (PCE).

  [See Segment Routing for Traffic Engineering.]

Juniper Extension Toolkit (JET)

- **BGP route service API supports programming routes with IP-IP encapsulation attributes (MX240, MX480, MX960, PTX1000, QFX5110, QFX5200, QFX10002, and QFX10008)**—Starting in Junos OS Release 21.2R1, you can use the BGP route service API to program BGP routes with IP over IP (IP-IP) encapsulation attributes. You can specify the tunnel type, the remote endpoint address, and the color of the route. Keep the following in mind:
  - The egress endpoint must be a unicast IPv4 address.
  - The colors encoded in tunnel_encap and extended_community must match.

- If the encapsulation ext_com and the tunnel attribute are both present, the egress endpoint must match the next-hop address.

To enable this feature, configure the `bgp-signal` option at the `[edit routing-options dynamic-tunnels tunnel-name]` hierarchy level. The rest of your dynamic tunnel CLI configuration does affect the functionality of the programmed tunnels.

[See dynamic-tunnels and JET APIs on Juniper EngNet.]

Junos Telemetry Interface

NOTE: For Routing Engine telemetry sensors supported by this platform, see Telemetry Sensor Explorer. If any Platform Forwarding Engine sensors have been added for this release, they are listed below

- **End-of-message notification for Routing Engine sensors (EX2300, EX4300, EX4300-MP, EX9200, MX240, MX960, MX10016, MX2010, MX2020, PTX1000, PTX3000, PTX10001, QFX5100, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we've introduced an end-of-message (EoM) Boolean flag for all Junos telemetry interface (JTI) Routing Engine sensors. The flag notifies the collector that the current wrap has completed for a particular sensor path. A wrap is a complete key-value data dump for all the leaves under a sensor path.

  The EoM flag also enables the collector to detect when the end of wrap occurs without having to compare stream creation timestamp values that the collector receives from the packets. Comparing timestamp values is costly time-wise and delays data aggregation.

  To use this feature with gRPC Network Management Interface (gNMI) transport or Remote Procedure Call (gRPC), retrieve the protobuf files from the relevant branch on the Juniper Networks download site:

  - GnmiJuniperTelemetryHeaderExtension.proto (gNMI)
  - agent.proto (for gRPC)

  For example: https://github.com/Juniper/telemetry/blob/master/20.3/20.3R1/protos/GnmiJuniperTelemetryHeaderExtension.proto.

  After you download and install the new protobuf files on a collector, the EoM field is present in the packets received.

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

- **Monitoring and optimizing Packet Forwarding Engine sensor data export (PTX Series and QFX Series)**—Starting in Junos OS Release 21.2R1, you can optimize Packet Forwarding Engine sensor data to dynamically determine how to export data as quickly as possible based on three sensor categories:

heavy data (dynamic scale), medium data (predicted scale), and low data (fixed scale). In addition, you can use our new sensor to retrieve export details of all Packet Forwarding Engine sensors. Use the resource path **/junos/system/linecard/export/monitor** to monitor export details for each subscribed Packet Forwarding Engine sensor including:

- Number of reaps
- Number of wraps (a complete data set)
- Number of packets sent
- Average number of reaps and wraps
- Timestamps for reaps and wraps

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

- **Enable VOQ utilization monitoring with JTI (PTX1000, PTX5000, PTX10000, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.2R1, you can enable the enable the export utilization data for CoS virtual output queues (VOQs) on aggregated Ethernet or physical Ethernet WAN interfaces. Using this feature, you can export peak buffer utilization data for a given queue with Junos telemetry interface (JTI). Monitoring this data can assist in preventing micro-bursts and high buffer utilization for a given queue because peak buffer utilization is transient and might not be reported by instantaneous queue depth.

  To enable monitoring, include `queue-monitoring enable` at one of the following hierarchies:

  - [`edit class-of-service interfaces` *`if-name`*]
  - [`edit class-of-service traffic-control-profiles` *`tcp-name`*]
  - [`edit class-of-service schedulers` *`scheduler-name`*]

  To export data to a collector, include the resource path **/junos/system/linecard/qmon-sw** in a subscription.

  [See queue-monitoring, show class-of-service interface, show class-of-service traffic-control-profile , show class-of-service scheduler-map and show interfaces voq *interface-name*.]

- **JTI: logical interface statistics for IPv4 and IPv6 family input and output counters (MX Series and PTX Series routers using third-generation FPCs)**—Starting in Junos OS Release 21.2R1, you can stream per-family logical interface statistics for IPv4 and IPv6 traffic using Junos telemetry interface (JTI) and Remote Procedure Calls (gRPC) to an outside collector.

  To access these sensors, use the resource paths **/junos/system/linecard/interface/logical/family/ipv4/usage/** and **/junos/system/linecard/interface/logical/family/ipv6/usage/** in a subscription.

[See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).]

Layer 2 VPN

- **Support for Layer 2 services on SR-TE tunnels using transport class (MX series, PTX Series, and vMX)**—Starting in Junos OS Release 21.2R1, you can configure the following Layer 2 services on colored and non-colored segment routing traffic engineer (SR-TE) tunnels using transport classes.

  - Layer 2 Circuits
  - Layer 2 VPN
  - BGP VPLS

  [See Layer 2 Circuit Overview ,**Introduction to Configuring Layer 2 VPNs**, and BGP Classful Transport Planes Overview .]

Network Management and Monitoring

- **sFlow support for IP-IP traffic with VRF (PTX1000, PTX10002, PTX10008, QFX10002, and QFX10008)**—Starting in Junos OS Release 21.2R1, you can use sFlow technology to sample IP over IP (IP-IP) traffic that is hosted on multiple virtual routing and forwarding (VRF) instances. sFlow sampling now reports the extended router data correctly when the incoming and outgoing interfaces of the traffic reside on two different VRFs in IP-IP traffic for egress sampling.

  [See Overview of sFlow Technology.]

- **Support for syslog over TLS (EX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, you can transport syslog (control plane) over Transport Layer Security (TLS) protocol. Encapsulating syslog over TLS allows you to:

  - Validate the remote destination (syslog server) before transmitting any sensitive syslog information. (Authentication)
  - Encrypt the syslog during the transport. (Encryption)
  - Verify that the data has not been modified or tampered with (Integrity)

  Before you enable this feature, ensure you:

  - Configure public key infrastructure (PKI) in Junos
  - Configure and load the digital certificates
  - Configure the remote destination (syslog server) that supports syslog over TLS

To enable transport of syslog (control plane) over TLS, use the `tls` statement at the [`edit system syslog host host-name transport`] hierarchy level.

Routing Options

- **Enhancements to prefix-limit and accepted-prefix-limit configuration statements, and updates to show bgp neighbor command (ACX1000, EX9200, MX Series, PTX5000, and QFX10002)**— Starting from Junos OS Release 21.2R1, the `prefix-limit` and `accepted-prefix-limit` configuration statements include the following options:

  - `drop-excess <percentage>`—If you include the `drop-excess <percentage>` option and specify a percentage, the excess routes are dropped when the number of prefixes exceeds the specified percentage.

  - `hide-excess <percentage>`—If you include the `hide-excess <percentage>` option and specify a percentage, the excess routes are hidden when the number of prefixes exceeds the specified percentage.

  The `show bgp neighbor` command has been enhanced to display the following additional information:

  - Count of prefixes that are dropped or hidden based on network layer reachability information (NLRI) when the maximum allowed prefixes threshold is exceeded.

  - Alerts when a peer starts to drop or hide routes.

  - Configuration details of the `prefix-limit` and `accepted-prefix-limit` configuration statements.

  [See prefix-limit, accepted-prefix-limit, show bgp neighbor, and Multiprotocol BGP.]

Routing Policy and Firewall Filters

- **Class-based firewall filters (PTX Series)**—Starting in Junos OS Release 21.2R1, you can apply firewall filter actions like drop, reject, sample, and police on packets classified by destination class usage (DCU) and source class usage (SCU) accounting, for example as part of a design to provide distributed denial-of-service (DDoS) protection to specific customers.

  [See Configuring the Filter Profile.]

Routing Protocols

- **Support for origin validation with BGP sharding (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, you can use origin validation with BGP sharding. You can configure `rib-sharding` with routing-options validation.

- **BMP with BGP sharding and update I/O (JRR Series, MX Series, PTX Series, and vMX)**—Starting in Junos OS Release 21.2R1, we support BGP Monitoring Protocol (BMP) with BGP sharding and update I/O in the multithreaded mode.

- **Basic MVPN support with BGP sharding (cRPD, JRR200, MX2020, PTX5000, and QFX10002)**—Starting in Junos OS 21.2R1, we support the basic multicast virtual private network (MVPN) functionalities with BGP sharding.

  > **NOTE**: Sharding is not supported for the MVPN address family.

- **Support for BGP SR-TE policy advertisement and error handling (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, if the SDN controller cannot directly install SR-TE routes on non-Juniper Networks devices, the controller installs the BGP SR-TE policy on the route reflector, which forwards the SR-TE routes to non-Juniper devices.

  To advertise SR-TE policy to non-Juniper devices, define a BGP policy that includes the `family inet-srte` statement at the `[edit policy-options policy-statement term from protocol bgp]` hierarchy level.

  To push an unlabeled IP packet before other labels, include the `inet-color-append-explicit-null`statement at the `[edit protocols source-packet-routing]`hierarchy level.

- **Support for BGP classful transport (CT) with underlying colored SRTE tunnels (MX Series and PTX Series with FPC-PTX-P1-A)**– Starting in Junos OS Release 21.2R1, BGP-CT can resolve service routes using the transport RIBs and compute the next-hop. Services currently supported over BGP-CT can also use the underlying SRTE colored tunnels for route resolution.

  To enable BGP CT service route resolution over underlying SRTE colored tunnels, include the `use-transport-class` statement at the `[edit protocols source-packet-routing]` hierarchy level.

  [See use-transport-class.]

- **Flexible algorithm inter-level leaking support for SRv6 and SR-MPLS in ISIS (ACX Series, MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support flexible algorithm inter-level leaking for SRv6 and SR-MPLS in IS-IS. Also, we partially support TE-App RFC 8919 in its basic form and extends 6PE support for flexible algorithm.

Services Applications

- **Support for hardware timestamping of Two-Way Active Measurement Protocol (TWAMP) and RPM probe messages (PTX5000)**—Starting in Junos OS Release 21.2R1, we've extended support for hardware timestamping of TWAMP and RPM probe messages. Hardware timestamping is enabled by default for TWAMP, but you must configure it for RPM. You use TWAMP and RPM to measure IP performance between two devices in a network. By configuring hardware timestamping for RPM, you can account for the latency in the communication of probe messages and generate more accurate timers in the Packet Forwarding Engine. To configure hardware timestamping for RPM, include the `hardware-timestamping` statement at the `[edit services rpm probe` *`probe-owner`* `test` *`test-name`*`]` hierarchy level.

[See Understanding Two-Way Active Measurement Protocol on Routers, Understanding Using Probes for Real-Time Performance Monitoring on M, T, PTX, and MX Series Routers, and Configuring RPM Timestamping on MX, M, T, and PTX Series Routers and EX Series Switches.]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Static route resolution over SR-TE tunnel (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we support static route resolution over segment routing–traffic engineered (SR-TE) colored and uncolored label-switched paths (LSPs). To enable this feature, configure the `spring-te-lsp-next-hop` statement at the `[edit routing-options static` *`destination`*`]` and `[edit routing-options rib` *`rib name`* `static` *`destination`*`]` hierarchy levels. The feature support extends towards static, DTM, BGP-SR-TE, and PCEP source types that are currently supported by Source Packet Routing in Networking–Traffic Engineering (SPRING-TE). If a source is not configured, by default, it takes the next hop as static.

  You must configure the `tunnel-tracking` statement at the `[edit protocols source-packet-routing]` hierarchy level to enable this feature. This feature enhances the accuracy of first-hop label-based tunnel status for SR-TE tunnels according to their route resolution.

  [See spring-te-lsp-next-hop and source-packet-routing.]

- **Express segments using SR-TE underlay (MX Series and PTX Series)**—Starting in Junos OS Release 21.2R1, we've introduced SR-TE underlay path support for express segments to enable end-to-end transport of segment routing–traffic engineered (SR-TE) label-switched paths (LSPs) for very large multi-domain networks. The path is automated using segment-set or template policies for uncolored or colored segment routing policies. The `rib-group` configuration is required to import addresses to inet.3 for colored segment routing policies. When the express segments underlay is colored SR-TE, you need to configure the `no-chained-composite-next-hop` statement at the `[edit protocols source-packet-routing]` hierarchy level for the express segment to install the correct flattened next hop.

  This feature has the following limitations:

  - When the express segments underlay is colored SR-TE, the express segment does not inherit the SR-TE LSP underlay attributes (SR-TE name, metric).
  - The `install-nexthop` option at the `[edit policy-options policy-statement policy-name term term-name then]` hierarchy level to filter a specific SR-TE LSP bu its name is not supported.
  - Express segments do not consider the respective weights of the primary and secondary segment lists of SR-TE LSP. Secondary LSP segments can be preferred for traffic even when the primary segment is up.

  [See Express Segment LSP Configuration.]

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.2R1

IN THIS SECTION

Class of Service (CoS)

- Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

EVPN

- **Support for displaying SVLBNH information**— You can now view shared VXLAN load balancing next hop (SVLBNH) information when you display the VXLAN tunnel endpoint information for a specified ESI and routing instance by using the `show ethernet-switching vxlan-tunnel-end-point esi` *`esi-identifier`* `esi-identifier instance` *`instance`* `svlbnh` command.

General Routing

- **SSH session connection limit and rate limit per connection (PTX Series and QFX Series)**— We have introduced SSH `connection-limit` and `rate-limit` options at the [`edit system services ssh`] hierarchy levels to enable SSH connection limit and rate limit per connection. The default connection limit value is 75 connections and there is no default value associated with rate limit.

- **Secure boot disabled alarm is raised (PTX10008)**— The `Secure boot disabled` alarm is raised when the system boots with secure boot disabled in bios.

- **Enhancement to the show chassis pic command (Junos OS)**—You can now view additional information about the optics when you run the `show chassis pic` command. The output now displays the following additional field: MSA Version: Multi-source Agreements (MSA) version that the specified optics is compliant to. Values supported are: SFP+/SFP28 — SFF-8472 (versions 9.3 - 12.3), QSFP+/QSFP28 — SFF 8363 (versions 1.3 - 2.10), and QSFP-DD — CMIS 3.0, 4.0, 5.0. Previously, the `show chassis pic` command did not display this additional field.

  [See show chassis pic.]

- **Enhancement to the show interfaces (Aggregated Ethernet) command (ACX Series, PTX Series, and QFX Series)**— When you run the `show interfaces extensive` command for ae interfaces. You can now view following additional fields for MAC statistics : Receive, Transmit, Broadcast and Multicast packets.

  [See show chassis pic.]

Interfaces and Chassis

- **Blocking duplicate IP detection in the same routing instance (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, and SRX Series)**—Junos will no longer accept duplicate IPs between different logical interfaces in the same routing instance. Refer to the table mentioned in the topic inet (interfaces). When you try to configure same IP on two logical interfaces inside same routing instance, the commit will be blocked with the error displayed as shown below:

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.2/24
[edit]
user@host# commit
commit complete
[edit]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 2.2.2.2/24
[edit]
user@host# commit
```

```
[edit interfaces ge-0/0/2 unit 0 family inet]
 'address 2.2.2.2/24'
 identical local address found on rt_inst [default], intfs [ge-0/0/2.0 and ge-0/0/1.0],
family [inet].
error: configuration check-out failed
```

[See inet(interfaces).]

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python op scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the device passes command-line arguments to a Python op script, it prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device prefixes a single hyphen (-) to all argument names.

  [See Declaring and Using Command-Line Arguments in Op Scripts.]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

  When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

  [See request system scripts refresh-from and cert-file (Scripts).]

Network Management and Monitoring

- **Chef and Puppet support removed (EX Series except EX4400, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, Junos OS products that were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS. FreeBSD 12.x based Junos OS does not support installing existing Chef or Puppet packages.

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a

hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See Creating Action Scripts for YANG RPCs on Devices Running Junos OS and Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules.]

- **Changes to <commit> RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server's response for `<commit>` operations includes the following changes:

  - If a successful `<commit>` operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.
  - The NETCONF server response emits the `<source-daemon>` element as a child of the `<error-info>` element instead of the `<rpc-error>` element.
  - If you also configure the `flatten-commit-results` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server suppresses any `<commit-results>` XML subtree in the response and only emits an `<ok/>` or `<rpc-error>` element.

  [See Configuring RFC-Compliant NETCONF Sessions.]

Known Limitations

IN THIS SECTION

Learn about known limitations 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.

Infrastructure

- To upgrade to Junos OS Release 21.2R1, you need to include the no-validate option when issuing the upgrade command.

  Junos OS releases prior to 20.4R1 do not support the no-validate option with unified ISSU. In order to upgrade from an older release to Junos OS Release 21.2R1 with unified ISSU, you must first upgrade to a release that supports the no-validate option for unified ISSU, such as 20.4R1. PR1568757

Open Issues

IN THIS SECTION

Learn about open issues 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.

General Routing

- On a PTX Series router with a third-generation FPC, an error message shows up when the FPC goes online or offline. PR1322491
- This is a timing issue during the sxe interface bring up (w.r.t i40e driver). This can be recovered by rebooting the complete board. PR1442249
- FIPS mode is not supported. PR1530951

- `Socket to sflowd closed` error comes up when the ukern socket to sflowd daemon (server) is closed. The error is rectified as the client successfully reestablishes the connection in the subsequent attempts. When these errors are consistent, it indicates a communication issue between sflowd and the sFlow running on the FPC. PR1538863

- 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

- Copying files to `/tmp/ causes a huge JTASK_SCHED_SLIP`. Copy files to `/var/tmp/` instead. PR1571214

- When firewall is configured with both discard and port-mirror as actions in the same term, mirrored packet will be corrupted (will have two l2 headers). PR1576914

- On PTX10008, the end-to-end traffic is not flowing for ethernet-switching in EP Style. PR1583219

- On PTX3000 platform, if RPD is thrashing while doing GRES switchover there may be traffic loss on MPLS LSPs. PR1590681

- Sflow Ingress sampling with ECMP export is not working due to TAL request failure for both single and double VLAN tagged traffic. Works fine without ECMP. PR1598263

- On PTX10008 and PTX10016 devices with LC1101, LC1102, and LC1103 line cards, interface flapping might cause the interface CRC errors increase continuously, then traffic loss might be seen. This is a rare timing issue. PR1600768

- The **RS Fatal** error (like "RS PHi Parity Fatal") is not handled in Chassis Management Error Handling Infrastructure (CMError) in Junos. Normally, the **RS Fatal** error is caused by hardware problem. If **RS Fatal** error happens on Packet Forwarding Engine (PFE) on FPC-PTX-P1-A/FPC2-PTX-P1A in PTX5000 or FPC-SFF-PTX-P1-A/FPC-SFF-PTX-T in PTX3000, any new operation on the FPC experiencing **RS Fatal** error will fail. For example, once any other FPC in the same chassis is rebooted and coming online, the FPC experiencing **RS Fatal** error will try to flush the virtual output queues (VOQs) towards the restarted FPC. However, the flush will fail due to the **RS Fatal** error and hence the buffers for VOQs towards the restarted FPC is not programmed. And this will result in traffic drops on all Packet Forwarding Engines of the problem FPC (even on the Packet Forwarding Engine not having "RS Fatal" error) towards the restarted FPC. PR1600935

- On PTX5000 platforms with QSFP-100GBASE-LR4 optics, after a software upgrade, link flaps might be observed momentarily due to a firmware upgrade issue. This issue might cause traffic impact. PR1606008

MPLS

- On all Junos platforms with NSR configured, when **dual-tranport** is configured under protocols ldp and the inet-lsr-id/inet6-lsr-id is different from the router-id, the Label Distribution Protocol (LDP) replication session might not get synchronized and causing traffic loss during Routing Engine switchover. PR1598174
- On all Junos platforms that is NSR configured, when configuration statement **dual-transport** is configured under **protocols ldp** and the inet-lsr-id/inet6-lsr-id is different from the router-id, VPLS connection on peer device might get down and traffic loss would occur during Routing Engine switchover. PR1601854

Routing Protocols

- Due to a race condition between route re-convergence and the BGP-PIC version up message to the Packet Forwarding Engine, after a remote transit router reboot, certain BGP routes might reuse stale LDP next hops and cause packet discard at the transit router during the route re-convergence window. PR1495435
- Here two routers with two different capacities are converging at two different times, so the micro loop occurs between the two nodes. So please check the work around provided. PR1577458

User Interface and Configuration

- When a user tries to deactivate the MPLS related configuration, the commit fails on backup Routing Engine. Work-around details are provided in the corresponding section below. PR1519367
- On PTX platforms, the default routing policy might not be changed back after it is changed to network-services enhanced mode. PR1587174

Resolved Issues

IN THIS SECTION

Learn about 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: 21.2R1

IN THIS SECTION

General Routing

- FPC reboot might be observed in the events of jlock hog more than 5 seconds. PR1439929

- The dcpfe crash might be seen on platforms with auto-channelization enabled. PR1484336
- Aggregate Ethernet interfaces do not display member links' statistic. PR1505596
- Error messages `t6e_dfe_tuning_state:et-6/0/0 - Failed to dfe tuning count 10` might be seen after links flap PR1512919
- Packet drops might be seen with all commit events with 1G speed configured interface. PR1524614
- The VM host platform might crash continuously after performing upgrade or downgrade and booting up with the new image. PR1544875
- On the PTX10000 platforms, traffic might get dropped when the set routing-options forwarding-table no-ecmp-fast-reroute configuration is changed to 128 ECMP entries. PR1547457
- WR Linux 6 platforms might get stuck after upgrading or downgrading image version and restarting device. PR1547669
- PTX1000 and PTX10002 platforms could get stuck after performing vmhost reboot post image upgrade. PR1548254
- On PTX3000 platform, the chassisd might crash with faulty SIB3.PR1551291
- The interface filter with source-port 0 matches everything instead of port 0. PR1551305
- Packet drop might happen on the aggregate Ethernet bundle which has the single child member only. PR1551736
- There might be traffic drop when default EXP classifier maps traffic to FC with no schedulers. PR1554266
- The micro BFD session might flap with DDoS policer. PR1557782
- The device might run out of service post GRES/ISSU. PR1558958
- Major alarms might be seen when a large class-of-service buffer-size is configured. PR1559459
- Traffic drop might be seen in 128 or more way ECMP paths after FPC restart. PR1559528
- The command `show system health-monitor` is hidden for PTX10000 platform. PR1560268
- In PTX10000 platform, `the command set chassis display` is hidden. PR1560453
- After recovering from restart routing immediately, object-info anomalies are observed on rpdagent. PR1561812
- On PTX10000, an enhancement to enable watchdog petting log on Line Cards.PR1561980
- The dcpfe process might crash in ECMP scenario. PR1564147

- Junos OS, upon receipt of specific packets BFD sessions might flap due to DDoS policer implementation in Packet Forwarding Engine (CVE-2021-0280). PR1564807
- On PTX10002-60C platform, another port will also shutdown after shutting down one port. PR1568294
- LLDP out-of-bounds read vulnerability in l2cpd. PR1569312
- Interface hold-time down feature might not work in certain conditions. PR1570204
- PTX1000 with unified disk fails netboot with `Timed out waiting for device dev-jvg_P-jlvmjunos.device` message. PR1571275
- The gRPC session hanging is in CLOSED state. PR1571999
- Channelized ports on PTX10002 platforms might drop traffic. PR1575742
- In PTX5000, you might observe traffic loss.PR1578511
- TACACS traffic might be dropped. PR1578579
- BFD sessions might flap during traffic spikes on PTX platforms. PR1578599
- Authentication might fail if the password contains special characters. PR1580003
- The IS-IS packet might be corrupted on the provider edge device over the Layer 2 circuit tunnel. PR1580047
- On PTX platforms, the traffic might drop. PR1580211
- The `clear synchronous-ethernet wait-to-restore interface` command not available. PR1581556
- On PTX5000 and PTX3000, configure and delete the FEC mode will disable the auto-FEC91 on an interface that uses QSFP28-SR4. PR1582200
- Junos telemetry Interfaces: Missing Leaves - Transceiver/state. PR1583076
- On PTX10008, `show chassis clocks` - should be handled in a meaningful error. PR1583715
- The packets might be dropped by Packet Forwarding Engine of PTX5000 after changing the queue of IEEE-802.1ad classifier on FPC-PTX-P1-A or FPC2-PTX-P1A. PR1584042
- On Junos OS, QFX Series and PTX Series; FPC resource usage increases when certain packets are processed which are being VXLAN encapsulated (CVE-2021-31361). PR1584197
- JDI-RCT: T/PTX, `Failed to get pechip handle for chip 0` and `prds_encap_sample_flood_lpbk_desc_install: Egress NH descriptor install OK for Flabel 7808` errors seen during bringup. PR1585594

- The na-grpc process crash might be seen and existing telemetry connections will be disconnected. PR1587956
- There might be higher latency in traffic flow than configured or default value. PR1588514
- In a telemetry scenario, the jsd process crash might be seen in rare situations. PR1589103
- On PTX3000 and PTX5000 platforms, the 40G and 100G interface might get stuck down after link flaps. PR1589170
- The Layer 2 circuit packets with destination mac 01:00:0c:cc:cc:cd may get punted. PR1601360

EVPN

- EVPN option is missing under [`edit routing-instances routing-instance-name protocols`] PR1581821

Forwarding and Sampling

- Junos OS, user-defined ARP Policer is not applied on Aggregated Ethernet (AE) interface until firewall process is restarted (CVE-2021-0289). PR1528403

General Routing

- On PTX10008, NSR Support for LDP/RSVP/BGP: BGP NH_index (indirect and unilist) change after GRES+NSR Trigger causing a momentary (unexpected) traffic loss. PR1560323

Infrastructure

- The kernel crash with core file might be seen if churn happens for a flood composite next hop. PR1548545
- The TCP session might fail on devices with dual Routing Engines. PR1555441
- Next-hop incorrectly associated with lo0 in forwarding-table when interface is configured as unnumbered. PR1570918

Layer 2 Ethernet Services

- The copying of files to the RCB over WAN ports is slow. PR1496895

MPLS

- MPLS-LIB memory leak might be seen in SR scenario. PR1556495

- Traffic sent over an LSP might be dropped if two consecutive PLRs along the LSP perform local repair and bypass protecting the second PLR fails. PR1566101
- The rpd process on the transit node might crash when MPLS traceroute on the ingress node is performed. PR1573517
- Sub-optimal routing issues might be seen in case LDP route with multiple next-hops. PR1582037

Multicast

- FPC might crash in a multicast scenario. PR1569957

Network Management and Monitoring

- The mib2d process crashes and generates a core dump on backup Routing Engine. PR1557384
- FPC crash might be observed in a scaled firewall configuration on PTX series platforms. PR1586817

Routing Policy and Firewall Filters

- Generated route goes to the hidden state when the protect core command is enabled. PR1562867

Routing Protocols

- The rpd might restart after interface flap if Layer2-map. PR1557710
- BGP LU session flap might be seen with the AIGP used scenario. PR1558102
- Traffic loss might occur for stitched traffic from SR towards LDP if no-eligible-backup is configured. PR1558565
- The ppmd memory leak might cause traffic loss. PR1561850
- Traffic loss might be observed due to the rpd crash in BGP multipath scenario. PR1568600
- BGP session carrying VPNv4 prefix with IPv6 next-hop might be dropped. PR1580578
- Process rpd crash might be seen in certain IS-IS scenario. PR1583484
- The rpd crash might be seen when BGP RPKI session record-lifetime is configured less than the hold-time. PR1585321
- BGP Egress-TE routes lose to BGP routes using the same protocol-preference. PR1593332

User Interface and Configuration

- The LACP might stop working after disabling LACP sync-reset. PR1576146

VPNs

- The rpd might crash during a race condition under BGP multipath scenario. PR1567918

Documentation Updates

There are no errata and changes in Junos OS Release 21.2R1 for the PTX Series documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading to Release 21.2

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 21.2R1:

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-
x86-64-21.2R1.9.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-
x86-64-21.2R1.9-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 21.2 jinstall package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the jinstall package that corresponds to the previously installed software.

NOTE: Most of the existing `request system` commands are not supported on routers with RE-PTX-X8 Routing Engines. See the VM Host Software Administrative Commands in the Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

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

Upgrading a Router with Redundant Routing Engines

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

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

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

Junos OS Release Notes for QFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 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

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

Dynamic Host Configuration Protocol

- **Relay agent information options for stateless DHCP relay (QFX Series)**—Starting in Junos OS Release 21.2R1, QFX Series switches support the configuration of relay agent information options for stateless DHCP relay. These options enable the relay agent to add information to DHCP client requests that the relay agent forwards to the DHCP server. The remote ID and circuit ID options are supported for both DHCPv4 and DHCPv6 stateless relay.

  [See DHCP Relay Agent.]

EVPN

- **EVPN Type 2 and Type 5 route coexistence (EX4650, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we support the coexistence of EVPN Type 2 and Type 5 routes in EVPN-VXLAN edge-routed bridging overlay fabrics. This feature enables more efficient traffic flow

and better usage of Packet Forwarding Engine resources. The switch applies a preference algorithm when you enable Type 5 routes. For any destinations for which the switch has no Type 5 route, the switch uses Type 2 routes by default. Otherwise, the switch gives preference to:

- Type 2 routes for local ESI interfaces (locally learned routes)
- Type 5 routes for all other destinations within the data center or across data centers

You can refine these preferences by configuring routing policies in the EVPN routing instance to control the Type 5 routes that the switch imports and exports.

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

- **Optimized inter-subnet multicast support with symmetric bridge domain configuration in an EVPN-VXLAN fabric (QFX5110, QFX5120, QFX10002-36Q, and QFX10002-72Q)**—Starting in Junos OS Release 21.2R1, you can configure optimized inter-subnet multicast (OISM) on leaf devices and border leaf devices in an EVPN-VXLAN edge-routed bridging overlay fabric. This feature helps optimize the routing of multicast traffic across VLANs in an EVPN tenant domain. This feature uses a supplemental bridge domain (SBD) and a multicast VLAN (MVLAN) to route multicast traffic from or to devices outside of the fabric. This feature also works with existing IGMP snooping and selective multicast (SMET) forwarding optimizations to minimize replication in the EVPN core when bridging within tenant VLANs.

  With this implementation, you must enable OISM and IGMP snooping on all the leaf and border leaf devices in the EVPN-VXLAN fabric. You also must configure the SBD and all tenant VLANs symmetrically on all leaf and border leaf devices in the fabric.

  You can use OISM with:

  - EVPN on the `default-switch` instance with VLAN-aware bundle service model (Layer 2)
  - Routing instances of type `vrf` (Layer 3)
  - EVPN single-homing or multihoming (all-active mode)
  - IGMPv2
  - Multicast sources and receivers within the EVPN data center
  - Multicast sources and receivers outside the EVPN data center that are reachable through the border leaf devices

  [See Optimized Inter-Subnet Multicast in EVPN Networks.]

- **Overlapping VLAN support for edge-routed bridging in an EVPN-VXLAN fabric (QFX5110 and QFX5120)**—Starting in Junos OS Release 21.2R1, you can map the host VLAN to the VLAN that is provisioned on the leaf device by using VLAN translation. The host VLAN is translated to the VLAN

that is already configured on the leaf device before the packet is processed. Conversely, the packet egresses from the access port with the translated VLAN.

[See vlan-rewrite.]

Forwarding Options

- **Remote port mirroring with VXLAN encapsulation (EX4650, QFX5120-32C, QFX5120-48T, and QFX5120-48Y switches)**—Starting in Junos OS Release 21.2R1, you can configure remote port mirroring in an EVPN-VXLAN environment. Remote port mirroring sends copies of packets to an output destination for remote monitoring. This feature supports VXLAN encapsulation of the mirrored packets so they can be sent to an output destination in a separate virtual network identifier (VNI) domain.

High Availability

- **Hardware-assisted inline BFD (QFX5120-32C and QFX5120-48Y)**—Starting in Junos OS Release 21.2R1, we support a hardware implementation of the inline BFD protocol in firmware form. The ASIC firmware handles most of the BFD protocol processing. The firmware uses existing paths to forward any BFD events that must be processed by protocol processes. The ASIC firmware processes the packets more quickly than the software, so hardware-assisted inline BFD sessions can have keepalive intervals of less than a second. These platforms support this feature for single-hop and multihop IPv4 and IPv6 BFD sessions.

  [See ppm and Bidirectional Forwarding Detection (BFD).]

Interfaces

- **Flexible Ethernet support (QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.2R1, you can configure flexible Ethernet services to support a Layer 2 bridging interface while simultaneously supporting other encapsulation options on the same physical interface. You can configure a physical or aggregate Ethernet interface to simultaneously support Layer 2 bridging, Layer 3 IP routing, and VLAN-based CCC connections.

  > **NOTE**: On QFX10000 line of Switches running Junos OS releases earlier than Release 21.2R1, we do not support configuring `vlan-bridge` and any other encapsulations on an interface that has `flexible-ethernet-services` enabled.

  [See Flexible Ethernet Services Encapsulation.]

Juniper Extension Toolkit (JET)

- **BGP route service API supports programming routes with IP-IP encapsulation attributes (MX240, MX480, MX960, PTX1000, QFX5110, QFX5200, QFX10002, and QFX10008)**—Starting in Junos OS

Release 21.2R1, you can use the BGP route service API to program BGP routes with IP over IP (IP-IP) encapsulation attributes. You can specify the tunnel type, the remote endpoint address, and the color of the route. Keep the following in mind:

- The egress endpoint must be a unicast IPv4 address.
- The colors encoded in tunnel_encap and extended_community must match.
- If the encapsulation ext_com and the tunnel attribute are both present, the egress endpoint must match the next-hop address.

To enable this feature, configure the `bgp-signal` option at the `[edit routing-options dynamic-tunnels` *`tunnel-name`*`]` hierarchy level. The rest of your dynamic tunnel CLI configuration does affect the functionality of the programmed tunnels.

[See dynamic-tunnels and JET APIs on Juniper EngNet.]

Junos Telemetry Interface

NOTE: For Routing Engine telemetry sensors supported by this platform, see Telemetry Sensor Explorer. If any Platform Forwarding Engine sensors have been added for this release, they are listed below

- **End-of-message notification for Routing Engine sensors (EX2300, EX4300, EX4300-MP, EX9200, MX240, MX960, MX10016, MX2010, MX2020, PTX1000, PTX3000, PTX10001, QFX5100, QFX5110, QFX5120, and QFX10002)**—Starting in Junos OS Release 21.2R1, we've introduced an end-of-message (EoM) Boolean flag for all Junos telemetry interface (JTI) Routing Engine sensors. The flag notifies the collector that the current wrap has completed for a particular sensor path. A wrap is a complete key-value data dump for all the leaves under a sensor path.

  The EoM flag also enables the collector to detect when the end of wrap occurs without having to compare stream creation timestamp values that the collector receives from the packets. Comparing timestamp values is costly time-wise and delays data aggregation.

  To use this feature with gRPC Network Management Interface (gNMI) transport or Remote Procedure Call (gRPC), retrieve the protobuf files from the relevant branch on the Juniper Networks download site:

  - GnmiJuniperTelemetryHeaderExtension.proto (gNMI)
  - agent.proto (for gRPC)

  For example: https://github.com/Juniper/telemetry/blob/master/20.3/20.3R1/protos/GnmiJuniperTelemetryHeaderExtension.proto.

After you download and install the new protobuf files on a collector, the EoM field is present in the packets received.

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

- **Monitoring and optimizing Packet Forwarding Engine sensor data export (PTX Series and QFX Series)**—Starting in Junos OS Release 21.2R1, you can optimize Packet Forwarding Engine sensor data to dynamically determine how to export data as quickly as possible based on three sensor categories: heavy data (dynamic scale), medium data (predicted scale), and low data (fixed scale). In addition, you can use our new sensor to retrieve export details of all Packet Forwarding Engine sensors. Use the resource path **/junos/system/linecard/export/monitor** to monitor export details for each subscribed Packet Forwarding Engine sensor including:

  - Number of reaps
  - Number of wraps (a complete data set)
  - Number of packets sent
  - Average number of reaps and wraps
  - Timestamps for reaps and wraps

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

- **Enable VOQ utilization monitoring with JTI (PTX1000, PTX5000, PTX10000, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.2R1, you can enable the enable the export utilization data for CoS virtual output queues (VOQs) on aggregated Ethernet or physical Ethernet WAN interfaces. Using this feature, you can export peak buffer utilization data for a given queue with Junos telemetry interface (JTI). Monitoring this data can assist in preventing micro-bursts and high buffer utilization for a given queue because peak buffer utilization is transient and might not be reported by instantaneous queue depth.

  To enable monitoring, include `queue-monitoring enable` at one of the following hierarchies:

  - [`edit class-of-service interfaces` *`if-name`*]
  - [`edit class-of-service traffic-control-profiles` *`tcp-name`*]
  - [`edit class-of-service schedulers` *`scheduler-name`*]

  To export data to a collector, include the resource path **/junos/system/linecard/qmon-sw** in a subscription.

  [See queue-monitoring, show class-of-service interface, show class-of-service traffic-control-profile , show class-of-service scheduler-map and show interfaces voq *interface-name*.]

Licensing

- **Juniper Agile Licensing (QFX5110-48S, QFX5110-32Q, QFX5120-32C, QFX5120-48T, and QFX5210-64C)**—Starting in Junos OS Release Evolved 21.2R1, the QFX switches support Juniper Agile Licensing.

  Juniper Agile Licensing provides simplified and centralized license administration and deployment. You can use Juniper Agile Licensing to install and manage licenses for software features.

  Juniper Agile Licensing supports soft enforcement of software feature licenses. With soft enforcement, if you configure a feature without a license, Junos OS displays a warning when you commit the configuration except for PTP feature. However, the feature is operational. In addition, Junos os generated periodic alarms indicating that you need the license to use the feature. You can see the list of alarms at System Log Explorer.

  Table 10 on page 238 describes the licensing support with use case examples for QFX5110-48S, QFX5110-32Q, QFX5120-32C, QFX5120-48T, and QFX5210-64C.

  Table 10: Supported Features on QFX5110-48S, QFX5110-32Q, QFX5120-32C, QFX5120-48T, and QFX5210-64C

QFX Switch License Model	Use Case Examples or Solutions	Detailed Features
Standard	Basic Layer 2 switching or basic Layer 3 forwarding	BFD, Filters (Layer 2 and Layer 3), Layer 2 (*x*STP, 802.1Q, LAG), Layer 3 (static), QoS (Layer 2 and Layer 3), and SNMP
Advanced	Data center fabric	**Advanced 1**: BGP, FBF, GRE, IGMP version 1, IGMP version 2, and IGMP version 3, IS-IS, JTI, MC-LAG, Multicast Listener Discovery (MLD) version 1, MLD version 2, OSPF, RIP, VRF and VRRP **Advanced 2**: Advanced 1 features, CFM, ESI-LAG, EVPN-VXLAN, Layer 3 multicast, OAM, PTP, Q-in-Q, and Virtual Chassis
Premium	Data center interconnect or data center edge	Advance Enterprise Features, EVPN-MPLS, Layer 2 circuit, Layer 3 VPN (MPLS), LDP, RSVP, Segment routing, and SR-TE

  In addition, you can install additional port bandwidth usage license to increase the port bandwidth usage.

  [See Flex Software License for QFX Switches, Juniper Agile Licensing Guide, and Configuring Licenses in Junos OS.]

Network Management and Monitoring

- **sFlow support for IP-IP traffic with VRF (PTX1000, PTX10002, PTX10008, QFX10002, and QFX10008)**—Starting in Junos OS Release 21.2R1, you can use sFlow technology to sample IP over IP (IP-IP) traffic that is hosted on multiple virtual routing and forwarding (VRF) instances. sFlow sampling now reports the extended router data correctly when the incoming and outgoing interfaces of the traffic reside on two different VRFs in IP-IP traffic for egress sampling.

  [See Overview of sFlow Technology.]

- **Support for syslog over TLS (EX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, you can transport syslog (control plane) over Transport Layer Security (TLS) protocol. Encapsulating syslog over TLS allows you to:

  - Validate the remote destination (syslog server) before transmitting any sensitive syslog information. (Authentication)
  - Encrypt the syslog during the transport. (Encryption)
  - Verify that the data has not been modified or tampered with (Integrity)

  Before you enable this feature, ensure you:

  - Configure public key infrastructure (PKI) in Junos
  - Configure and load the digital certificates
  - Configure the remote destination (syslog server) that supports syslog over TLS

  To enable transport of syslog (control plane) over TLS, use the `tls` statement at the [`edit system syslog host host-name transport`] hierarchy level.

Routing Options

- **Enhancements to prefix-limit and accepted-prefix-limit configuration statements, and updates to show bgp neighbor command (ACX1000, EX9200, MX Series, PTX5000, and QFX10002)**— Starting from Junos OS Release 21.2R1, the `prefix-limit` and `accepted-prefix-limit` configuration statements include the following options:

  - `drop-excess <percentage>`—If you include the `drop-excess <percentage>` option and specify a percentage, the excess routes are dropped when the number of prefixes exceeds the specified percentage.
  - `hide-excess <percentage>`—If you include the `hide-excess <percentage>` option and specify a percentage, the excess routes are hidden when the number of prefixes exceeds the specified percentage.

  The `show bgp neighbor` command has been enhanced to display the following additional information:

- Count of prefixes that are dropped or hidden based on network layer reachability information (NLRI) when the maximum allowed prefixes threshold is exceeded.
- Alerts when a peer starts to drop or hide routes.
- Configuration details of the `prefix-limit` and `accepted-prefix-limit` configuration statements.

[See prefix-limit, accepted-prefix-limit, show bgp neighbor, and Multiprotocol BGP.]

Routing Protocols

- **Basic MVPN support with BGP sharding (cRPD, JRR200, MX2020, PTX5000, and QFX10002)**—Starting in Junos OS 21.2R1, we support the basic multicast virtual private network (MVPN) functionalities with BGP sharding.

  NOTE: Sharding is not supported for the MVPN address family.

Services Applications

- **Support for MPLS, MPLS-IPv4, and MPLS-IPv6 inline active flow monitoring (QFX10002-60C)**—Starting in Junos OS Release 21.2R1, you can perform inline active flow monitoring for MPLS, MPLS-IPv4, MPLS-IPv6, and MPLS-over-UDP traffic. For MPLS-over-UDP flows, inline active flow monitoring allows you to look past the tunnel header to sample and report on the inner payload, at both the transit and egress nodes of the tunnel. We support IPFIX and version 9 templates but only ingress sampling.

  [See Inline Active Flow Monitoring of MPLS-over-UDP Flows.]

Software Installation and Upgrade

- **Dynamic port speed detection for ZTP (QFX10002)**—Starting in Junos OS Release 21.2R1, you can use either WAN interfaces or management interfaces to automatically download and install the appropriate software and the configuration file on your device during the bootstrap process. Zero-touch provisioning (ZTP) automatically configures WAN interfaces based on the optics type, and then connects your device to the DHCP server to perform the bootstrap process.

  [See Zero Touch Provisioning.]

System Management

- **Support for PTP SMPTE media profile (QFX5120-48T)**—Starting in Junos OS Release 21.2R1, you can enable the Society of Motion Picture and Television Engineers (SMPTE) profile to support video applications to enable capture, video edit, and playback to be used in professional broadcast environments. The standard allows multiple video sources to stay in synchronization across various equipment by enabling time and frequency synchronization to all devices.

[See Understanding the PTP Media Profiles and Configuring the PTP Media Profiles.]

- **Support for PTP boundary clock and enterprise profile (QFX5120-48T)**—Starting in Junos OS Release 21.2R1, you can enable the boundary clock and enterprise profiles, which are based on Precision Time Protocol (PTP) version 2 (PTPv2). The PTP enterprise profile enables the enterprise and financial markets to add a timestamp to the operations of different systems, and to handle a range of latencies and delays. The boundary clock has multiple network connections and can act as a source (primary) and a destination (client) for synchronization messages. It synchronizes itself to a best primary clock through a client port and supports synchronization of remote clock clients to it on primary ports.

  [See Understanding the Precision Time Protocol Enterprise Profile and IEEE 1588v2 PTP Boundary Clock Overview.]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for QFX Series Switches.

What's Changed in Release 21.2R1

IN THIS SECTION

Class of Service (CoS)

- **[edit class-of-service traffic-control-profiles] should be ordered-by system as per customers**—Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

- Starting with Junos OS Release 21.2, Junos OS displays class of service configuration in alphabetical order regardless of configuration order.

EVPN

- **Support for displaying SVLBNH information**—You can now view shared VXLAN load balancing next hop (SVLBNH) information when you display the VXLAN tunnel endpoint information for a specified ESI and routing instance by using `show ethernet-switching vxlan-tunnel-end-point esi` *`esi-identifier`* `esi-identifier instance` *`instance`* `svlbnh` command.

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python op scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the device passes command-line arguments to a Python op script, it prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device prefixes a single hyphen (-) to all argument names.

  [See Declaring and Using Command-Line Arguments in Op Scripts.]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

  When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

  [See request system scripts refresh-from and cert-file (Scripts).]

Platform and Infrastructure

- **SSH session connection limit and rate limit per connection (PTX Series and QFX Series)**—We have introduced SSH `<connection-limit>` and `<rate-limit>` options at the `<edit system services ssh>` hierarchy levels to enable SSH connection limit and rate limit per connection. The default connection limit value is 75 connections and there is no default value associated with rate limit.

- **Support only for manual channelization on QSFP-100G-SR4-T2 optics (QFX5120-48T and QFX5120-32C)**—We recommend that you use the active optical cable (AOC) for auto-channelization. The QSFP-100G-SR4-T2 cables do not support auto-channelization. To use the QSFP-100G-SR4-T2 optics with an external breakout cable, you must configure the channelization manually by running the `<channel-speed>` statement at the `edit chassis fpc slot-number pic pic-number (port port-number | port-range port-range-low port-range-high)` hierarchy level.

- **Juniper Agile Licensing (QFX5120-48Y, QFX5110-32Q, and QFX5110-48S)—**Starting from this release onwards, the QFX switch supports following features:

  - **Standard:**BFD, Filters (Layer 2 and Layer 3), Layer 2 (xSTP, 802.1Q, LAG), Layer 3 (static), QoS (Layer 2 and Layer 3), and SNMP

  - **Advanced 1:** Standard features, BGP, IS-IS, FBF, VRRP, MC-LAG, Layer 3 (static), GRE tunnel, OSPF, RIP, sFlow, and Virtual Chassis

  - **Advanced 2:** Advanced 1 features, CFM, Q-in-Q, VXLAN, PCEP, ESI-LAG, Timing, Ethernet OAM, EVPN-VXLAN, IGMP version 1, IGMP version 2, and IGMP version 3, PIM, and Multicast Listener Discovery (MLD) version 1 or version 2

  - **Premium:** Advanced 2 features, Layer 3 VPN, LDP, RSVP, Layer 2 circuit, EVPN-MPLS, Segment routing, MPLS, and MACsec

  [See Flex Software License for QFX Series Switches and Juniper Agile Licensing Guide.]

Layer 2 Ethernet Services

- **Link selection support for DHCP (QFX Series)**—We've introduced `link-selection` statement at the `edit forwarding-options dhcp-relay relay-option-82` hierarchy level, which allows DHCP relay to add suboption 5 to option 82. Suboption 5 allows DHCP proxy clients and relay agents to request an IP address for a specific subnet from a specific IP address range and scope. Earlier to this release, the DHCP relay drops packets during the renewal DHCP process as the DHCP Server uses the leaf's address as a destination to acknowledge DHCP renewal message.
  [See relay-option-82.]

Network Management and Monitoring

- **Chef and Puppet support removed (EX Series except EX4400, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.2R1, Junos OS products that were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS. FreeBSD 12.x based Junos OS does not support installing existing Chef or Puppet packages.

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

  [See Creating Action Scripts for YANG RPCs on Devices Running Junos OS and Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules.]

- **Changes to `<commit>` RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server's response for `<commit>` operations includes the following changes:

  - If a successful `<commit>` operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.

  - The NETCONF server response emits the `<source-daemon>` element as a child of the `<error-info>` element instead of the `<rpc-error>` element.

  - If you also configure the `flatten-commit-results` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server suppresses any `<commit-results>` XML subtree in the response and only emits an `<ok/>` or `<rpc-error>` element.

  [See Configuring RFC-Compliant NETCONF Sessions.]

Known Limitations

IN THIS SECTION

Learn about known limitations 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.

Platform and Infrastructure

- Junos OS can hang trying to acquire the SMP IPI lock while rebooting when it is running as a VM on Linux and QEMU hypervisor. Device can be recovered using power-cycle of the device PR1385970
- On QFX10002 line of switches, issue occurs due to the PECHIP limitation when you tag the underlay. After de-encapsulation, when the inner packet recirculates, the packets retains the VLAN tag property from the outer header since the outer header was tagged. Thus, 4 bytes of inner tag gets overwritten in the inner packet and gets corrupted resulting in EGP checksum trap in PECHIP. A workaround has been added to enable the `ncapsulate-inner-vlan` statement. PR1435864
- On QFX10002 platform, for sFlow egress sampling on an AE interface under Dynamic IPIP tunnel transit scenario, the nextHop field will not be present in the sFlow export data. PR1533307
- On QFX5100 devices not running the qfx-5e codes (non-TVP architecture), when an image with the Broadcom SDK upgrade (6.5.x) is installed, the CPU utilization may go up by around 5%. PR1534234
- RPD core dump is observed at device reboot and/or daemon restart time. Daemon recovers and there is no service impact on routing protocol usage. Impact: Feature usage reporting for scale based licensed features in routing area will not be reported. Junos-Evolved based PTX products have scale based routing features and hence are impacted due to this issue. Junos bassed QFX and EX products do not have scale based routing features and hence are not impacted due to this issue. PR1567043
- On QFX10002-72Q devices, configuration validation is not supported during an image downgrade or upgrade. PR1579050

Routing Protocols

- On QFX5120-48YM platform, when scale of IPv4 and IPv6 routes are present in LPM profile, few of the IPv6 routes will not be installed when the ports on which routes are learnt is flapped due to LPM table full error. PR1557655

Open Issues

IN THIS SECTION

Learn about open issues 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.

Platform and Infrastructure

- On a PTX Series router or QFX10000 switch with a third-generation FPC, an error message is displayed when the FPC goes online or offline. PR1322491
- QFX10K: Source MAC and TTL values are not updated for routed multicast packets in EVPN-VXLAN PR1346894
- You can observe a timing issue when the sxe interface start (regarding i40e driver). You can be recover this state by rebooting the complete board. PR1442249
- storm-control does not rate-limit ARP packets on QFX10K although shutdown action works PR1461958
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- When running the `show pfe filter hw filter-name` *`filter name`* command, the command fails to retrieve the PFE programming details of the filter. PR1495712
- The issue occurs if you try to call delete for one family and add/change for another family with a higher number of filter terms which requires either expansion of the filter or creation of a new filter on a fully scaled system where different families of CLI filters utilize all the slices. The Packet Forwarding Engine fails to add the new filter as we are getting messages out of sequence. It means the add/change of filter is called earlier than the delete of another filter that will free up the slices. PR1512242

- MSDP sessions might reset after a GRES reset even when nonstop routing (NSR) state is synchronized and ready for switchover PR1526679
- The "Socket to sflowd closed" error comes up when the ukern socket to sflowd daemon (server) is closed. The error rectifies itself as the client successfully reestablishes the connection in the subsequent attempts. When these errors are consistent, it indicates a communication issue between sflowd and the sFlow running on the FPC. PR1538863
- EVPN-VxLAN: vmcore generates core file on master and backup Routing Engine of QFX10k8 with Layer 2/Layer 3 multicast configuration. PR1539259
- 100G AOC from Innolight does not comes up after multiple reboots.It recovers after interface enable/disable PR1548525
- Users cannot subscribe to any path that ends with "key". PR1553534
- 5M DAC connected between QFX10002-60C and MX2010 doesn't link up. But with 1M and 3M DAC this interop works as expected. It is to be noted QFX10002-60C and ACX Series routers or traffic generator the same 5M DAC works seamlessly. There seems to be a certain SI or link level configuration on both QFX10002-60C and MX2010. It needs to be debugged with the help from hardware and SI teams and resolved. PR1555955
- In Release 20.2, some features will show up as a licensed feature. Customers might see alarms, commit warnings and "show system license" output as below. However, there would be no functional impact. PR1558017
- On the QFX5120 line of switches, amber LEDs are displayed for the fan modules after upgrading to Junos OS Release 20.2R1. PR1558407
- To avoid the additional interface flap, interface hold time needs to be configured. PR1562857
- Starting in Junos 21.1R1, Junos will be shipping with python3 (python2 is no longer supported). In ZTP process, if a python script is being downloaded, please ensure the python script follows python3 syntax (there are certain changes between python2 and python3 syntax). Also, so far (ie until 20.4R1), the python script had #!/usr/bin/python as the first line (ie the path of the python interpreter). The same needs to be changed to #!/usr/bin/python3 from 21.1R1. PR1565069
- The chassisd logs floods with "pic_create_ifname: 0/0/0 pic type F050 not supported" messages for every connected port. The flooding might happen every few seconds. PR1566440
- BUM traffic replication over VTEP is sending out more packets than expected. There seems to be a loop also in the topology. PR1570689
- When soft loopback port and analyzer configurations are committed together, hardware might not get programmed with the analyzer. This issue is not seen when physical loopback is used to achieve the same. PR1581542

- When physical loopback is used and both the ports are with EP style in the same RSPAN VLAN, it might lead to flooding. PR1581876
- RPD core file is seen @rt_iflnh_set_nhid. Core file is due to assertion caused by failure of hbt_insert for nhid belonging to a logical interface. It is seen that there is a duplicate entry present which causes the hbt_insert failure. PR1588128
- 'input ingress' and 'input egress' together for the same port will not work in mirroring with VXLAN encapsulation. PR1589854
- Verification of filter counter statistics failed as received packets are doubled. PR1590009
- On QFX5k with EVPN-VxLAN, the dcpfe core may be observed in one of the LEAF device in steady state after performing 'clear ethernet-switching table' on remote SPINE device in. PR1593950

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 21.2R1

IN THIS SECTION

Class of Service (CoS)

- Dscp classifier doesn't work and all packets are sent to single queue. PR1585361

EVPN

- On the QFX10000 devices, the l2ald process generates the core file at l2ald_VXLAN_ifl_create_event_handler at /src/junos/usr.sbin/l2ald/platform/junos/l2ald_rtsock_VXLAN.c:477. PR1560068
- global-mac-ip-table-aging-time; change from a high to low value might not take effect. PR1562925
- dev-longevity l2ald cored @ l2ald_next_bd_member. PR1570757

Forwarding and Sampling

- The configuration archive transfer-on-commit fails when running Junos OS Release 18.2R3-S6.5. PR1563641

Interfaces and Chassis

- MAC address entry issue might be observed after the MC-LAG interface. PR1562535

Layer 2 Features

- On the QFX5110-32Q line of switches, LACP does not come up in the Non-Oversubscribed mode for a set of ports. PR1563171
- On the QFX5120 devices, packets with VLAN ID 0 are dropped. PR1566850
- MAC addresses learnt from MC-LAG client device might keep flapping between the ICL interface and MC-AE interface after one child link in MC-AE interface is disabled. PR1582473

Layer 2 Ethernet Services

- DHCP packet drop might be seen when the DHCP relay is configured on a leaf device. PR1554992

Platform and Infrastructure

- Console access on backup VC member is not allowed. PR1530106
- FPC might crash in a scaled-firewall configuration. PR1586817
- On the QFX5000 line of switches, the egress ACL filter entries is only 512 in Junos OS Release 19.4R1. PR1472206
- On the QFX10000 device, the chassisd process might generate core files on the backup Routing Engine after commit for 200 seconds due to the following error message: CHASSISD_MAIN_THREAD_STALLED. PR1481143
- The OSPF neighborship gets stuck in the Start state after configuring the EVPN-VXLAN. PR1519244
- Layer 3 classifier takes effect though the Layer 2 classifier is configured. PR1520570
- Some inter-VLAN traffic flows do not converge after rebooting a spine (QFX10002) device in an EVPN-VXLAN non-collapsed scaled scenario. PR1522585
- Packet drops might be seen with all commit events with 1G speed configured interface. PR1524614
- Traffic loss might be observed on interfaces in a VXLAN environment. PR1524955
- On the QFX5100 Virtual Chassis and Virtual Chassis fan, after NSSU while performing GRES, backup can generate core file and go to the database prompt. PR1533874
- The dcpfe process might crash and cause FPC to restart due to the traffic burst. PR1534340
- The interfaces on QFX5100-48T switch might stay up when the peer device is rebooting. PR1538071
- The BFD neighborship fails with the EVPN_VXLAN configuration after the Layer 2 learning restarts. PR1538600
- On the QFX10000 devices, the dcpfe process might crash in the specific MAC move cases and traffic loss might be observed in the EVPN-VXLAN scenario. PR1542709
- FPC(s) may fail to come online when the corresponding power is restored afterward but not present during the power-up stage. PR1545838
- OSPFv3 session might keep flapping and OSPFv3 hellos might be dropped in the host path. PR1547032

- On QFX10000 device, traffic might get dropped when the set routing-options forwarding-table no-ecmp-fast-reroute configuration is changed to 128 ECMP entries. PR1547457
- On the QFX10000 devices, you need to move WRL7 SDK to RCPL31. PR1547565
- The 40GbE interface might be channelized after restarting the Virtual Chassis member. PR1548267
- The interface filter with source-port 0 matches everything instead of port 0. PR1551305
- On the QFX5000 devices, the ARP resolution might fail. PR1552671
- The interface might not come up with 1G optics. PR1554098
- Traffic might not passed due to the addition of the VLAN tag 2 while passing through the Virtual Chassis port. PR1555835
- QFX10002-72Q SNMP walk jnxOperatingEntry show only two PSU even four PSU installed. PR1555852
- Traffic might be dropped when a firewall filter rule uses the then VLAN action. PR1556198
- The dcpfe process might crash and restart with a dcpfe core file created while running the Type5 EVPN-VXLAN with 2000 VLANs. PR1556561
- DHCP Discover packets are not getting flooded with VXLAN configuration. PR1557049
- The MAC addresses learned in a Virtual Chassis may fail aging out in MAC scaling environment. PR1558128
- On the QFX5000 devices, the firewall filter might fail. PR1558320
- On the QFX5120 device, amber LEDs are displayed for the fan modules after upgrading to Junos OS Release 20.2R1. PR1558407
- On the QFX5110 devices, untagged traffic routed over native-vlan might be dropped. PR1560038
- PRBS (Pseudo Random Binary Sequence) test on the QFX5200 devices fails for 100GbE interfaces with the default settings. PR1560086
- Few IPv6 ARP ND fails after loading the base configurations. PR1560161
- On the QFX5120-48Y devices, the Layer 3 IPv4 traffic issue is observed after loading the non-collapsed type 5 EVPN-VXLAN configuration. PR1560173
- When configuring the static MAC and static ARP on the EVPN core aggregate interface, the underlay next-hop programming might not be updated in the Packet Forwarding Engine. PR1561084
- The tunable optics SFP+-10G-T-DWDM-ZR doesn't work on EX/QFX devices. PR1561181

- PTP BC with G.8275.2.enh profile_2 512 clients does not come up. PR1561348
- PTP lock status gets stuck at the Acquiring state instead of the Phase Aligned state. PR1561372
- Firewall filters might not work after unified ISSU. PR1561690
- On the QFX10000 devices, the dcpfe process might crash during the configuration changes. PR1561746
- Traffic loss might occur in a large-scaled EVPN scenario when the next-hop type changes between discard and unicast. PR1562425
- On the QFX5000 devices, port mirroring might not work as expected. PR1562607
- QFX5110-48s-4c :: ptp traffic-statistics are not as expected. PR1563876
- Output of "show chassis fpc ether-types" command includes FPC slot number. PR1564496
- The PFE telemetry data might not be streamed out in QFX-VC. PR1566528
- On the QFX5100 device, the following internal comment is displayed: Placeholder for QFX platform configuration. PR1567037
- rpd core at boot time of a device. PR1567043
- On the QFX10002 devices, discrepancy in inet.1 versus Packet Forwarding Engine reports multicast routes. PR1567353
- QFX10K: Firewall log incorrectly populating from PFE for IPv6 traffic. PR1569120
- PTP management message with SMTLV is sent only to the first port number to go active in the member multicast-mode l2-ifl. PR1571283
- Unexpected packet loss might happen if subunit of the physical interface is deleted. PR1571286
- DCI traffic loss of 100% observed in transit spine devices. PR1572238
- Traffic loss might be observed due to dcpfe crash on QFX10002/QFX10008 platforms. PR1572889
- A high rate of 802.3X Pause Frames are sent out of the Interfaces on QFX10k. PR1575280
- The dual-speed supported DAC cable (100G to 4x25G Splitter) might not come up on QFX5120-48Y. PR1576180
- TACACS traffic might be dropped. PR1578579
- The dcpfe process crashes while checking the virtual tunnel-nh packet status. PR1580114
- When having analyzers mapped to channelized port then the mirror may not happen properly. PR1580473

- Kernel issue is observed in telemetry when the set services analytics streaming-server <> <> configuration is present and server is not reachable. PR1581192
- The switchover might be affected with the shared VXLAN tunnel. PR1581524
- The l2ald process generates the core file in l2ald_vxlan_ifl_create_event_handler while running the EVPN-VXLAN scripts in VQFX during the PCT submission. PR1582128
- pciephy and firmware download not working after migration to 6.5.19. PR1582244
- QFX10K Firewall Filter logs are incorrectly populated with entries for protocol 8847. PR1582780
- IRB:ping through irb interface is not working. PR1582989
- Port-Mirror : When delete AE member(s) then its NOT getting deleted (mirror trunk group) in the hardware for Analyzer input AE. PR1589579

Routing Protocols

- The fxpc process might crash after flapping the related protocols in the ECMP scenario. PR1556224
- BGP LU session flap might be seen with the AIGP used scenario. PR1558102
- On the QFX5110 devices, the ARP resolution might fail if native-vlan-id is configured on the VXLAN interface. PR1563569
- The dcpfe process might crash when the size of the Local Bias Filter Bitmap string exceeds 256 characters. PR1568159
- The untagged packets might not work on EX Series platforms. PR1568533
- The GRE egress traffic might not be forwarded between the different routing-instances. PR1573411
- The DHCP packets might be dropped by the QFX5000 in the Static VXLAN scenario. PR1576168
- The dcpfe process might crash when any interface flaps. PR1579736
- The rpd process might crash after committing with the configured static group 224.0.0.0 PR1586631
- On the QFX5000 line of switches, the egress ACL filter entries is only 512 in Junos OS Release 19.4R1. PR1472206
- On the QFX10000 device, the chassisd process might generate core files on the backup Routing Engine after commit for 200 seconds due to the following error message: CHASSISD_MAIN_THREAD_STALLED. PR1481143
- The OSPF neighborship gets stuck in the Start state after configuring the EVPN-VXLAN. PR1519244

- Layer 3 classifier takes effect though the Layer 2 classifier is configured. PR1520570
- Some inter-VLAN traffic flows do not converge after rebooting a spine (QFX10002) device in an EVPN-VXLAN non-collapsed scaled scenario. PR1522585
- Traffic loss might be observed on interfaces in a VXLAN environment. PR1524955
- On the QFX5100 Virtual Chassis and Virtual Chassis fan, after NSSU while performing GRES, backup can generate core file and go to the database prompt. PR1533874
- The dcpfe process might crash and cause FPC to restart due to the traffic burst. PR1534340
- The interfaces on QFX5100-48T switch might stay up when the peer device is rebooting. PR1538071
- The BFD neighborship fails with the EVPN_VXLAN configuration after the Layer 2 learning restarts. PR1538600
- On the QFX10000 devices, the dcpfe process might crash in the specific MAC move cases and traffic loss might be observed in the EVPN-VXLAN scenario. PR1542709
- FPC(s) may not boot-up on MX960/EX9214 in a certain condition. PR1545838
- OSPFv3 session might keep flapping and OSPFv3 hellos might be dropped in the host path. PR1547032
- On QFX10000 device, traffic might get dropped when the set routing-options forwarding-table no-ecmp-fast-reroute configuration is changed to 128 ECMP entries. PR1547457
- On the QFX10000 devices, you need to move WRL7 SDK to RCPL31. PR1547565
- The 40GbE interface might be channelized after restarting the Virtual Chassis member. PR1548267
- The interface filter with source-port 0 matches everything instead of port 0. PR1551305
- On the QFX5000 devices, the ARP resolution might fail. PR1552671
- Traffic might not passed due to the addition of the VLAN tag 2 while passing through the Virtual Chassis port. PR1555835
- QFX10002-72Q SNMP walk jnxOperatingEntry show only two PSU even four PSU installed. PR1555852
- Traffic might be dropped when a firewall filter rule uses the then VLAN action. PR1556198
- The dcpfe process might crash and restart with a dcpfe core file created while running the Type5 EVPN-VXLAN with 2000 VLANs. PR1556561
- DHCP Discover packets are not getting flooded with VXLAN configuration. PR1557049

- The MAC addresses learned in a Virtual Chassis may fail aging out in MAC scaling environment. PR1558128
- On the QFX5000 devices, the firewall filter might fail. PR1558320
- On the QFX5120 device, amber LEDs are displayed for the fan modules after upgrading to Junos OS Release 20.2R1. PR1558407
- On the QFX5110 devices, untagged traffic routed over native-vlan might be dropped. PR1560038
- PRBS (Pseudo Random Binary Sequence) test on the QFX5200 devices fails for 100GbE interfaces with the default settings. PR1560086
- Few IPv6 ARP ND fails after loading the base configurations. PR1560161
- On the QFX5120-48Y devices, the Layer 3 IPv4 traffic issue is observed after loading the non-collapsed type 5 EVPN-VXLAN configuration. PR1560173
- When configuring the static MAC and static ARP on the EVPN core aggregate interface, the underlay next-hop programming might not be updated in the Packet Forwarding Engine. PR1561084
- The tunable optics SFP+-10G-T-DWDM-ZR doesn't work on EX/QFX devices. PR1561181
- PTP BC with G.8275.2.enh profile_2 512 clients does not come up. PR1561348
- PTP lock status gets stuck at the Acquiring state instead of the Phase Aligned state. PR1561372
- Firewall filters might not work after ISSU. PR1561690
- On the QFX10000 devices, the dcpfe process might crash during the configuration changes. PR1561746
- Traffic loss might occur in a large-scaled EVPN scenario when the next-hop type changes between discard and unicast. PR1562425
- On the QFX5000 devices, port mirroring might not work as expected. PR1562607
- QFX5110-48s-4c :: ptp traffic-statistics are not as expected. PR1563876
- Output of "show chassis fpc ether-types" command includes FPC slot number. PR1564496
- The PFE telemetry data might not be streamed out in QFX-VC. PR1566528
- On the QFX5100 device, the following internal comment is displayed: Placeholder for QFX platform configuration. PR1567037
- rpd core at boot time of a device. PR1567043

- On the QFX10002 devices, discrepancy in inet.1 versus Packet Forwarding Engine reports multicast routes. PR1567353
- QFX10K: Firewall log incorrectly populating from PFE for IPv6 traffic. PR1569120
- PTP management message with SMTLV is sent only to the first port number to go active in the member multicast-mode l2-ifl. PR1571283
- Unexpected packet loss might happen if subunit of the physical interface is deleted. PR1571286
- DCI traffic loss of 100% observed in transit spine devices. PR1572238
- Traffic loss might be observed due to dcpfe crash on QFX10002/QFX10008 platforms. PR1572889
- A high rate of 802.3X Pause Frames are sent out of the Interfaces on QFX10k. PR1575280
- The dual-speed supported DAC cable (100G to 4x25G Splitter) might not come up on QFX5120-48Y. PR1576180
- The dcpfe process crashes while checking the virtual tunnel-nh packet status. PR1580114
- When having analyzers mapped to channelized port then the mirror may not happen properly. PR1580473
- Kernel issue is observed in telemetry when the set services analytics streaming-server <> <> configuration is present and server is not reachable. PR1581192
- The switchover might be affected with the shared VXLAN tunnel. PR1581524
- The l2ald process generates the core file in l2ald_vxlan_ifl_create_event_handler while running the EVPN-VXLAN scripts in VQFX during the PCT submission. PR1582128
- pciephy and firmware download not working after migration to 6.5.19. PR1582244
- QFX10K Firewall Filter logs are incorrectly populated with entries for protocol 8847. PR1582780
- Port-Mirror : When delete AE member(s) then its NOT getting deleted (mirror trunk group) in the hardware for Analyzer input AE. PR1589579

User Interface and Configuration

- The configuration under groups stanza is not inherited properly. PR1529989
- set chassis fpc 0 ether-type only applicable for ether index 6 to 27. PR1565695

Documentation Updates

There are no documentation errata or changes for the QFX Series switches in Junos OS Release 21.2R1.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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-x86-64-21.2R1.9.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-x86-64-21.2R1.9.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-x86-64-21.2R1.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-
x86-64-21.2R1.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-
x86-64-21.2R1.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-
x86-64-21.2R1.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:

- "Preparing the Switch for Software Installation" on page 267
- "Upgrading the Software Using Unified ISSU" on page 268

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

- Ensure that nonstop active routing (NSR), nonstop bridging (NSB), and graceful Routing Engine switchover (GRES) are enabled. NSB and GRES enable NSB-supported Layer 2 protocols to synchronize protocol information between the master and backup Routing Engines.

  To verify that nonstop active routing is enabled:

  NOTE: If nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

  ```
  user@switch> show task replication
          Stateful Replication: Enabled
          RE mode: Master
  ```

  If nonstop active routing is not enabled (`Stateful Replication` is `Disabled`), see *Configuring Nonstop Active Routing on Switches* for information about how to enable it.

- Enable nonstop bridging (NSB). See *Configuring Nonstop Bridging on Switches (CLI Procedure)* for information on how to enable it.

- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the `request system snapshot` command.

Upgrading the Software Using Unified ISSU

This procedure describes how to upgrade the software running on a standalone switch.

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in *Installing Software Packages on QFX Series Devices*.
2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:
   - On the switch, enter:

     ```
     user@switch> request system software in-service-upgrade /var/tmp/package-name.tgz
     ```

     where *package-name*.tgz is, for example, `jinstall-host-qfx-10-f-x86-64-20.4R1.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

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.

Junos OS Release Notes for SRX Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 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

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

Application Identification (AppID)

- **TLS version 1.3 support for SSL proxy (SRX Series)**—Starting in Junos OS Release 21.2R1, Secure Sockets Layer (SSL) proxy supports the Transport Layer Security (TLS) protocol version 1.3, which provides improved security and better performance. TLS version 1.3 supports the following cipher suites:
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256

- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256

[See SSL Proxy.]

- **Application-based multipath routing (AMR) improvements (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, SRX550 HM, and vSRX)**—Starting in Junos OS release 21.2R1, we've introduced the following improvements for AMR:
  - Support for the traffic in reverse direction
  - Queuing mechanism for out-of-order packets at the receiving device
  - Association of AMR rules and service-level agreement (SLA) rules with advanced policy-based routing (APBR) rule in an APBR profile
  - Link selection option that includes overlay interfaces such as GRE and secure tunnel
  - Enablement of AMR in one of the two modes—SLA violation mode or standalone mode
  - Support for IPv6 traffic
  - Support for AMR over IPsec and GRE sessions

  [See Application-Based Multipath Routing.]

- **Multicast support in SD-WAN deployments (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX4100, SRX4200, SRX4600, vSRX)**—Starting in Junos OS Release 21.2R1, we've added support for multicast traffic on SRX Series devices in Provider Edge (PE) for SD-WAN deployments. The support for multicast traffic is available when the security device is operating with forwarding option set as flow-based.

  Support for multicast traffic results in bandwidth preservation and more efficient traffic flows.
  See [mode (Security Forwarding Options) and Virtual Routing and Forwarding Instances in SD-WAN Deployments].

- **SLA link preference enhancement (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, SLA link preference for security device interfaces supports custom link tags. You can define the link preferences using the `preferred-tag` and `affinity` options.

  This enhancement allows application traffic to switch from a lower-priority link to a higher-priority link that meets SLA requirements.

  [See Understanding Link-Type Affinity for the Preferred Link and sla-rule.]

- **Application-based load balancing support for APBR (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, security devices support application-based load balancing for advanced policy-based routing (APBR). The APBR achieves load balancing by moving the application traffic in multiple WAN links using user-defined link selection criteria. The link selection criteria for application traffic depends on the link tag and link priority preference settings you defined for the advanced policy-based routing (APBR) interface. The application traffic distribution through the selected links depends on the link weight configuration.

  This feature improves the application traffic distribution performance for APBR and application quality of experience (AppQoE).

  [See Advanced Policy-Based Routing, sla-options, and interface.]

Authentication and Access Control

- **Unified policy support for firewall user authentication (SRX Series and vSRX)**—Starting in Junos OS Release 21.2R1, we support firewall user authentication in a security policy with dynamic applications (unified policy). You can configure pass-through or web authentication in the unified policy to restrict or permit users to access network resources.

  Firewall user authentication support in the unified policy provides an additional layer of protection in a network with dynamic traffic changes.

  [See Configure Firewall User Authentication with Unified Policies.]

- **Display dynamic-applications and URL category hit counts in a security policy (NFX Series and SRX Series)**—Starting in Junos OS Release 21.2R1, we've enhanced the `show security policies hit-count` command to include the dynamic applications and URL categories options. You can now display the utility rate of the policy according to the number of hits for the dynamic applications and URL categories.

  [See show security policies hit-count.]

- **Support to configure boot order (SRX1500 and SRX4600)**—Starting in Junos OS Release 21.2R1, you can choose to reboot your security devices from a USB device without power cycling. Use the `request system reboot usb` configuration statement to reboot your device from USB. This statement allows your security devices to detect a new USB device with a soft reboot.

  [See request system reboot usb (SRX Series).]

Flow-Based and Packet-Based Processing

- **TCP proxy short-circuit (SRX Series)**—Starting in Junos OS Release 21.2R1, for a session with an active TCP proxy plug-in, the SRX Series device disables TCP proxy if there is no further requirement for the TCP proxy plug-in based on the user-defined configuration or the state of the flow. This enhancement significantly improves the session flow performance.

- **Automated Express Path+ (SRX4600, SRX5400, SRX5600, and SRX5800)**—To enable Express Path+ (formerly known as services offloading) in releases before Junos OS Release 21.2R1, administrators need to manually define individual policies that they want to accelerate with network processing (NP) ASICs. Starting in Junos OS Release 21.2R1, administrators can use automated Express Path+ on the listed SRX Series devices to automatically offload all the eligible sessions to the ASIC network processors. This enhancement significantly improves the session flow performance.

  Automated Express Path+ requires underlying network processor cache (NP-cache) infrastructure. Starting in Junos OS Release 21.2R1, we've enabled NP-cache by default on the SRX5000 line of devices. Before this release, the SRX4600 had NP-cache enabled by default.

  [See Express Path.]

- **GRE acceleration enhancement (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.2R1, security devices support the existing PMI and GRE acceleration for non software-defined WAN (SD-WAN) deployments.

  PMI and GRE acceleration improve GRE and MPLS-over-GRE performance.

  [See gre-performance-acceleration and show security flow status.]

- **Multicast support in SD-WAN deployments (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, we've added support for multicast traffic on security devices in Provider Edge (PE) for SD-WAN deployments. The support for multicast traffic is available when the security device is operating with forwarding option set as flow-based.
  Support for multicast traffic results in bandwidth preservation and more efficient traffic flows.

  [See mode (Security Forwarding Options) and Virtual Routing and Forwarding Instances in SD-WAN Deployments.]

- **Support for logging and session-close reasons (SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4200, SRX4600, cSRX, and vSRX)**—Starting in Junos OS Release 21.2R1, we've enhanced the logging feature with support for the following flow functions:

  - Log for session-update
  - Support for 64-bit unified session-id
  - Adding new session close reason in session-close log

  We’ve introduced a CLI command `log session-update` that you can use to update the session details.

  [See Information Provided in Session Log Entries for SRX Series Services Gateways.]

Interfaces

- **MRU support (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.2R1, you can configure maximum receive unit (MRU) size to accept packet sizes which are bigger than the configured MTU size and configure different values for both MTU and MRU to prevent frequent fragmentation and reassembly of larger packets on the receiving side. You can configure MRU on the `xe`, `ge`, `et`, and `reth` interfaces.

  Use the CLI command `mru` under the `[edit interfaces` *`name`* `gigether-options]` hierarchy level to configure the MRU size in bytes.

  [See mru.]

J-Web

- **Enhanced Monitor and IPsec VPN pages (SRX Series)**—Starting in Junos OS Release 21.2R1, we've refreshed the following pages to provide a better experience for you:

  Monitor:

  - Network is the first submenu.
  - Interfaces and DHCP Server Binding are available under Monitor > Network.
  - IPsec VPN menu is available under Monitor > Network to display IKE and IPsec VPN security associations (SAs) and statistics information.

  IPsec VPN:

  - VPN menu is available under the Network tab.
  - The new Remote Access column displays remote URLs for Juniper Secure Connect.
  - Use **Add** to add a zone when you create or edit a Site-to-Site or Remote Access VPN tunnel interface.

  [See Monitor IPsec VPN, About the IPsec VPN Page, and Create a Site-to-Site VPN.]

- **Enhanced dashboard (SRX Series)**—Starting in Junos OS Release 21.2R1, we've enhanced Dashboard with new widgets to provide a better experience for you:

  - Threat Map—Displays the antivirus and IPS events data of the last one hour
  - NAT—Displays the top 10 source and destination translation hits
  - C&C Server and Malware Source Locations—Displays data of the last one hour
  - Incidents By Severity—Displays the top four incidents of data from the last one hour

- IPsec VPNs (IKE Peers)—Displays the count of IPsec VPN (IKE peers)

[See Dashboard Overview.]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **DNS DGA and tunnel detection (SRX Series)**—Starting in Junos OS Release 21.2R1, you can configure DNS Domain Generation Algorithm (DGA) detection and DNS tunnel detection. This feature enables you to block the malicious domains and DNS-tunneled requests or responses generated by infected hosts and command-and-control (C&C) servers. DGA periodically generates a large number of domain names that are used as rendezvous points (RPs) with their C&C servers. DNS tunneling is a cyberattack method that encodes the data of malicious programs or protocols in DNS queries and responses.

  Use the `set security-metadata-streaming policy` *`policy-name`* `detections dga` and `set security-metadata-streaming policy` *`policy-name`* `detections tunneling` commands at the `[edit services]` hierarchy to configure DNS DGA and tunneling detections.

  [See security-metadata-streaming.]

Junos Telemetry Interface

NOTE: For Routing Engine telemetry sensors supported by this platform, see Telemetry Sensor Explorer. If any Platform Forwarding Engine sensors have been added for this release, they are listed below

- **New Packet Forwarding Engine core CPU utilization sensor (SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, you can stream Packet Forwarding Engine core CPU utilization sensor data using Junos telemetry interface (JTI) and Remote Procedure Calls (gRPC) to an outside collector.

  To access this sensor, use the resource path **/junos/security/spu/cpu/usage/** in subscriptions.

  [See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).]

Network Management and Monitoring

- **SOAM support (SRX380, SRX300, SRX320, SRX340, SRX345, and SRX550HM)**—Starting in Junos OS Release 21.2R1, you can send delay measurement packets when a CFM session is established on SRX Series devices. We support performance monitoring MIBs that are necessary to manage Service Operation, Administration, and Maintenance (SOAM) performance monitoring functions that are defined in:

  - Service OAM requirements and framework specified by MEF 17

- Service OAM Performance Monitoring requirements as specified by SOAM-PM
- Service OAM management objects as specified by MEF 7.1
- Technical Specification MEF 36

[See Enterprise-Specific SNMP MIBs Supported by Junos OS.]

Software Installation and Upgrade

- **Support of the PXE boot method (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.2R1, we support the Preboot Execution Environment (PXE) boot method. With a PXE boot server, you can prepare an environment to boot devices by using a network interface that is independent of available data storage devices or installed operating systems. A client-enabled system uses a PXE boot to load an OS from a remote server and boot from it. PXE boot uses the standard protocols UDP/IP, Trivial File Transfer Protocol (TFTP), and BOOTP to transfer the image.

  [See Upgrading the Personality of a Device by Using a PXE Boot Server.]

Securing GTP and SCTP Traffic

- **Support for rate limiting based on APN-controlled aggregate rate limiting (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**–Starting in Junos OS Release 21.2R1, you can apply rate limiting for specific access point names (APNs) by using APN-controlled aggregate rate limiting (ARL). You can also configure APN groups and attach these groups to the GPRS tunneling protocol (GTP) profile for ARL. Configure the `apn-control` statement at the `[edit security gtp]` hierarchy level to enable the various configurations of APN-controlled ARL.

  [See profile (Security GTP), apn-control (Security GTP), apn-control-group (Security GTP), gtp, show security gtp profile, show security gtp counters, and show security gtp.]

VPNs

- **AutoVPN PSK support (SRX5000 line of devices with SPC3 card and vSRX running iked)**—To enable the VPN gateway to use a different IKE preshared key (PSK) for authenticating each remote peer, use the new CLI commands `seeded-pre-shared-key` *`ascii-text`* or `seeded-pre-shared-key` *`hexadecimal`* under the `[edit security ike policy` *`policy_name`*`]` hierarchy level. See policy.

  The SRX5000 line of devices with an SPC3 card and vSRX supports AutoVPN PSK only if the junos-ike-package is installed.

  To enable the VPN gateway to use the same IKE PSK for authenticating all remote peers, use the existing CLI commands `pre-shared-key` *`ascii-text`* or `pre-shared-key` *`hexadecimal`*.

  We also introduce an optional configuration to bypass the IKE ID validation. Use the `general-ikeid` configuration statement under the `[edit security ike gateway` *`gateway_name`* `dynamic]` hierarchy level to

bypass the IKE ID validation. If you enable this option, then during authentication of the remote peer, the SRX Series device and vSRX skips the IKE ID validation, and accepts all IKE ID types (hostname, user@hostname). See general-ikeid.

[See AutoVPN on Hub-and-Spoke Devices and Example: Configuring AutoVPN with Pre-Shared Key.]

- **Simplified packet drop identification for IPsec VPN services (SRX1500, SRX320, SRX340, SRX345, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 21.2R1, you can trace packet drop information without committing the configuration by using the `monitor security packet-drop` operational command for IPsec VPN services. This command includes various filters to generate the output fields according to your requirement.

  [See monitor security packet-drop.]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for SRX Series.

What's Changed in Release 21.2R1

IN THIS SECTION

Interfaces and Chassis

- Unable to Upgrade a Chassis Cluster Using In-Service Software Upgrade (SRX5400)— In chassis cluster mode, the backup router's destination address for IPv4 and IPv6 routers using the commands `edit system backup-router address destination destination-address` and `edit system inet6-backup-router address destination destination-address` must not be same as interface address configured for IPv4 and IPv6 using the commands `edit interfaces interface-name unit logical-unit-number family inet address ipv4-address` and `edit interfaces interface-name unit logical-unit-number family inet6 address ipv6-address`.

  [See Troubleshooting Chassis Cluster Management Issues.]

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python op scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the device passes command-line arguments to a Python op script, it prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device prefixes a single hyphen (-) to all argument names.

  [See Declaring and Using Command-Line Arguments in Op Scripts.]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

  When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

  [See request system scripts refresh-from and cert-file (Scripts).]

Network Management and Monitoring

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to

handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

[See Creating Action Scripts for YANG RPCs on Devices Running Junos OS and Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules.]

- **Changes to <commit> RPC responses in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—When you configure the rfc-compliant statement at the [edit system services netconf] hierarchy level, the NETCONF server's response for <commit> operations includes the following changes:

  - If a successful <commit> operation returns a response with one or more warnings, the warnings are redirected to the system log file, in addition to being omitted from the response.
  - The NETCONF server response emits the <source-daemon> element as a child of the <error-info> element instead of the <rpc-error> element.
  - If you also configure the flatten-commit-results statement at the [edit system services netconf] hierarchy level, the NETCONF server suppresses any <commit-results> XML subtree in the response and only emits an <ok/> or <rpc-error> element.

  [See Configuring RFC-Compliant NETCONF Sessions.]

- **New output field added in show pfe statistics traffic command (SRX380)**—Starting in Junos OS Release, you'll see Unicast EAPOL in the output of the show pfe statistics traffic command.

  [See show-pfe-statistics-traffic.]

VPNs

- **View the traffic selector type for an IPsec tunnel (SRX Series and MX Series)**—You can run the show security ipsec security-associations detail command to display the traffic selector type for a VPN. The command displays proxy-id or traffic-selector as a value for the TS Type output field based on your configuration.

  [See show-security-ipsec-security-associations.]

- **Deprecating Dynamic VPN CLI configuration statements and operational commands (SRX Series Devices)**—Starting in Junos OS Release 21.4R1, we'll be deprecating the dynamic VPN remote access solution. This means that you cannot use Pulse Secure Client on these devices.

  As part of this change, we'll be deprecating the [edit security dynamic-vpn] hierarchy level and its configuration options. We'll also be deprecating 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 this release for SRX Series devices.

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

General Routing

- Due to enhancements in AppID starting Junos OS Release 21.1R1, database files are not compatible with earlier releases. Hence, this issue is expected to be seen during downgrade from Junos OS Release 21.1R1 to earlier releases. PR1554490

Infrastructure

- The Junos OS Release 21.2R1 is stable12 BSD release. There is a limitation where image validation is not supported across different BSD versions. Image validation will fail from stable11 to stable12 for upgrade between different BSD releases. Use no-validate option when upgrading the Junos OS releases. PR1568757

VPNs

- In SPC2 and SPC3 mixed-mode HA deployments, tunnel per second (TPS) is getting affected while dead peer detection (DPD) is being served on existing tunnels. This limitation is due to a large chunk of CPU being occupied by infrastructure (gencfg) used by IKED to synchronize its DPD state to the backup nodes. PR1473482

Open Issues

Learn about open issues in this release for SRX Series devices.

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

Flow-Based Packet-Based Processing

- On SRX5000 line of devices with power-mode-ipsec enabled, the encap success received from PMI path packet might not show correct value output. PR1599044

General Routing

- SRX 1500 Services Gateway generates chassis alarms related to the TSensor and fan tray. PR1352281
- The show pfe statistics traffic command displays wrong output. To check the statistics use the show pfe statistics command. PR1566065
- When the device is downgraded to a release earlier than Junos OS Release 21.1 and then upgraded again to Junos OS Release 21.1, the appiddb tables might not get populated properly and have 0 entries. For such cases, after upgrading, uninstall and reinstall signature package. PR1567199
- For Junos OS release 21.2R1, when flapping IS-IS by disabling and enabling IS-IS protocols continuously for more than 5 times on SRX5000 line of devices, the IS-IS adjacency will not be recovered with gr interface. PR1572209
- HTTP sessions takes approximately 10 minutes to re-establish after a link flap between hub and spoke devices. PR1577021
- HA AP mode on-box logging in logical systems and tenant systems, intermittently security log contents of binary log file in logical systems are not as expected. PR1587360
- 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 might affect the application identification for the Web proxy session traffic. PR1588139
- On SRX345 device, ICMP checksum error and packet drops are observed while doing rapid ping on vdsl interface with MTU 1514. PR1591230
- In Junos OS release 20.3R3, sometimes on reboot log files are not getting generated. PR1594377
- Sometimes, when Jflow v9 flow record can contain wrong application id from cache, which can lead wrong identification of traffic application. PR1595787
- AAMW functions will be bypassed on HTTPs after AppID package upgraded to version 3313 or later in Junos OS release 21.2R1. PR1597179

- In Junos OS release 20.3R3, 21.1R2, and 21.2R1 the phone home ZTP is failing on SRX Series devices as phone home client is unable to connect to Phone Home Server or Redirect Server. PR1598462
- Intermittently the trace messages are not logged on sending multicast traffic. PR1598930

J-Web

- UI lists the IPsec VPNs information for uncommitted IPsec VPNs configuration under Monitor -> Netwrok -> IPsec VPN. PR1576609
- For Dynamic VPN configuration, topology is shown as Site to Site or Hub and Spoke under Monitor -> Network -> IPsec VPN page. PR1597889

Routing Policy and Firewall Filters

- The issue is related to output of one of the CLI command where it display some additional then expected data. However, it will not cause any issue with data path functionality on Packet Forwarding Engine. PR1582344

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
- 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
- In Layer 3 HA setup, core files are generated if you configure firewall to drop esp packets after the link encryption tunnel is up. PR1573102
- The certificate identifier length is incorrect in certain cases and this issue is seen in the CA certificate show command output show security pki ca-certificate detail. PR1589084
- On SRX Series devices, when site-to-site IPsec VPN is configured with traffic-selectors, if the VPN peer initiates an IKE negotiation using source-port other than 500, and at the same time, the IPsec IKE rekey (For the same VPN tunnel as the previous VPN peer initiates) occurs on the SRX Series device, the kmd process might crash. PR1596103

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 21.2R1

IN THIS SECTION

Application Layer Gateways (ALGs)

- On all SRX Series devices, if the SIP ALG is enabled, a core file might be generated. PR1555817

Chassis Clustering

- Disabled node on chassis cluster sent out ARP request packets. PR1548173
- SPU pause might be seen under GPRS tunneling protocol scenario. PR1559802

Flow-Based and Packet-Based Processing

- Instability with RGs on cluster. PR1550637
- The usp_max_tcplib_connection is not expected on SRX1500, SRX4100, and SRX4200 devices. PR1563881
- On the SRX platforms, the flowd or srxpfe process might crash when clearing the TCP-Proxy session. Traffic loss might be seen during the flowd or srxpfe process crash and restart. PR1573842
- On SRX Series devices, the filter from-zone has been added to the utility monitor security packet-drop. PR1574060

Forwarding and Sampling

- The configuration archive transfer-on-commit fails when running Junos OS Release 18.2R3-S6.5. PR1563641

General Routing

- The flowd process might generate core files frequently on SRX340. PR1463689
- Packet drops might be seen with all commit events with 1G speed configured interface. PR1524614
- The JNH memory leak could be observed on MPCs or MICs. PR1542882
- The output of the command show services application-identification group detail incorrectly included Micro-Applications (Micro-Apps) in the output of every group. PR1544727
- The kmd process might stop when the interface flaps. PR1544800
- SRX1500 reports fans running at over speed. PR1546132
- On SRX4100 and SRX4200 devices, if PEM0 is removed, the output of jnxOperatingDescr.2 command might be incomplete. PR1547053

- PKI CMPv2 client certificate enrollment does not work on SRX when using root-CA. PR1549954
- SRX4600 device might reset and fail to boot due to a failure accessing Solid State Drive (SSD). PR1551047
- On SRX1500, SRX-SFP-1GE-T (Part#740-013111) for a copper cable might be corrupted after reboot. PR1552820
- The speed mismatch error is seen while trying to commit reth0 with gigether-options. PR1553888
- Application identity unknown packet capture utility does not function on SRX Series devices when enhanced-services mode is enabled. PR1558812
- The show security log report top session-close group-by application order-by risk top-number 8 where-application-risk high xml encapsulation structure changed and caused script fail. PR1559013
- The show security log report top idp group-by threat-severity order-by count top-number 5 where-attack command display changes. PR1560027
- The PIC in SRX5K-SPC3 or MX-SPC3 card might get stuck in offline status after flowd process stops on it. PR1560305
- The pkid process runs at 100 percent when the device is unable to connect to a particular URL. PR1560374
- The DNS commands might not be executed and any new configuration might not take effect on connecting the SRX Series device to Juniper Sky ATP. PR1561169
- The show security log report top session-close group-by application order-by risk top-number 8 where-application-risk high xml encapsulation changed. PR1561286
- The idpd process might stop when committing IDP configuration under logical systems and tenant systems during RGs failover. PR1561298
- Fabric probe packets might be processed incorrectly when power-mode-ipsec is enabled. PR1564117
- The flowd process might pause and generates a core dump if JFlow version 9 is configured. PR1567871
- Wi-Fi mPIM on SRX Series devices is reaching out to NTP and DNS servers. PR1569680
- Missing snmp operation state method for power distribution module on SRX5800 and MX960 devices. PR1570433
- MACsec not using network-control queue. PR1571977

- Traffic going through the VRRP interface might be dropped when VRRP enabled IRB interface goes down. PR1572920
- In certain conditions on SRX Series devices, the timer values are updated for an existing fast BFD session, it may cause a fast BFD session deletion on the Packet Forwarding Engine. This will result in BFD session remaining down or Packet Forwarding Engine generates core files occasionally. PR1578946
- The ipfd process might stop and generate a core file when SecProfiling thread feeds are fetched from policy enforcer. PR1582454
- On SRX1500 device with AE interface configured, if the IRB interface is also configured and enabled, the srxpfe process might stop. PR1582989
- The 1G interfaces might not come up after device reboot. PR1585698
- On all Junos OS devices, the l2ald process pause could be observed on changing the routing-instance from VPLS to non-L2 routing-instance, with same routing-instance name is being used for both VPLS and non-L2 routing-instance. PR1586516
- On SRX Series devices, the protocol-version command which controls TLS versions (1.1, 1.2, 1.3, etc) within SSL proxy are unhidden. PR1587149
- On SRX Series devices, the unknown packet-capture functionality will no longer record SSL. UNKNOWN flows by default. This behavior can be changed by enabling the set services application-identification packet-capture ssl-unknown command. Without configuration the ssl-unknown command, the SRX Series devices will only capture flows marked as UNKNOWN or INCONCLUSIVE. PR1587875
- On SRX Series devices, the pass-through traffic on secure web proxy might fail after rebooting the device. PR1589957

Interfaces and Chassis

- When SRX Series devices receive proxy ARP requests on VRRP interfaces, SRX Series devices send ARP replies with the underlying interface MAC address. PR1526851
- Backup Routing Engine or backup node might get stuck in bad status with improper backup-router configuration. PR1530935
- The configuration check out failed with error message: identical local address found on rt_inst [default], intfs. PR1581877

Intrusion Detection and Prevention (IDP)

- The greater than or less than symbols are allowed for age-of-attack filter of dynamic attack group configuration. The age-of-attack field in signatures will be changed to CVE dates from activation dates. PR1397599
- IDP now supports the ability to create dynamic-attack-groups based on attack-prefix wildcards. PR1537195
- Adding signature in packet drop reason and sending to record packet drops module. PR1574603
- The IDP policy process might become unresponsive and fail to compile the IDP policy after an IDP automatic update. PR1577684

J-Web

- J-Web GUI does not allow you to save a rule if the cumulative shared objects are more than 2500 before the policy grid is saved. When there are several shared objects, there will be a noticeable delay in opening sources and destinations of a rule, and performing the rule action. PR1540047
- When the commit pending changes message is shown on the J-Web GUI, the contents of other messages, landing page, or pop-ups will not be clearly visible. PR1554024
- To improve performance in Monitoring > Network > Interfaces page, Admin Status is removed, services and protocols data merged into one host inbound traffic. PR1574895

Network Address Translation (NAT)

- Incorrect IPv6 UDP checksum inserted after translation of packet from IPv4 to IPv6, when IPv4 packet did not have a UDP checksum. PR1596952

Network Management and Monitoring

- The mib2d process crashes and generates a core files on backup Routing Engine. PR1557384
- SSH connection might become unresponsive and logs show kern.maxfiles limit exceeded by uid messages. PR1567634

Platform and Infrastructure

- The show chassis errors command is not supported on SRX5000 line of devices with RE3 and SCB3 installed. PR1560562

- The show chassis ethernet-switch errors command unexpectedly shows error counters for port 14 on the SRX5800 device. PR1563978
- On SRX5000 line of devices, the power budget calculation incorrectly assumes that all SCB cards contain a Routing Engine (RE). Hence, the available power budget is incorrectly decreased by 90W for each SCB which does not contain an RE. PR1568183
- There is a limitation where image validation might cause an MGD core thus causing ISSU to abort. This is due to incompatible BSD releases. PR1590099

Routing Policy and Firewall Filters

- The junos-defaults construct within a unified-policies application match criteria now restricts the ports and protocols of a flow on a per-dynamic-application basis. PR1551984
- SecIntel connection name resolution errors due to SecIntel memory leaks. PR1566128
- Traffic loss might be seen when a big number of applications or addresses is referenced by one policy. PR1576038

Unified Threat Management (UTM)

- UTM license expiry event lost might cause the device can't quit in advance service mode and the maximum-sessions is decreased by half. PR1563874

VPNs

- Traffic that goes through policy-based IPsec tunnel might be dropped after RG0 failover. PR1550232
- The iked process might stop with Multinode High Availability setup. PR1559121
- The pkid process generates core files while you do auto-enrollment of local certificates. PR1564300
- When there are multiple IPsec SAs, backup SA starts IPsec rekey. PR1565132
- The iked process might crash by operational commands on the SRX5000 line of devices with SRX5000-SPC3 card installed. PR1566649
- On all SRX Series devices and NFX350, if IPsec tunnels are configured with configuration payload VPN, they might not come up if the configured subnet mask on st0 is not equal to /8, /16 or /24. PR1593408

Documentation Updates

There are no errata and changes in Junos OS Release 21.2R1 for the SRX Series documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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 19,4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.1.

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.

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

Junos OS Release Notes for vMX

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 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

Learn about new features introduced in the Junos OS main and maintenance releases for vMX.

Layer 2 VPN

- **Support for Layer 2 services on SR-TE tunnels using transport class (MX series, PTX Series, and vMX)**—Starting in Junos OS Release 21.2R1, you can configure the following Layer 2 services on colored and non-colored segment routing traffic engineer (SR-TE) tunnels using transport classes.
  - Layer 2 Circuits
  - Layer 2 VPN
  - BGP VPLS

  [See Layer 2 Circuit Overview ,**Introduction to Configuring Layer 2 VPNs**, and BGP Classful Transport Planes Overview .]

Routing Options

- **Forwarding class counters support for `flat-file-profile` (MX Series and vMX)**—Starting in Junos OS Release 21.2R1, the `flat-file-profile` statement supports forwarding class counters. You can now switch from the ingress CoS queue counters configuration to the forwarding class counters configuration. To enable the forwarding class counters feature, configure the `use-fc-ingress-stats` statement at the [`edit accounting-options flat-file-profile` *`profile-name`*] hierarchy level.

  [See flat-file-profile (Accounting Options).]

Routing Protocols

- **BMP with BGP sharding and update I/O (JRR Series, MX Series, PTX Series, and vMX)**—Starting in Junos OS Release 21.2R1, we support BGP Monitoring Protocol (BMP) with BGP sharding and update I/O in the multithreaded mode.

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for vMX.

What's Changed in Release 21.2R1

IN THIS SECTION

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python op scripts (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the device passes command-line arguments to a Python op script, it prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device prefixes a single hyphen (-) to all argument names.

  [See Declaring and Using Command-Line Arguments in Op Scripts.]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

  When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under

the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See request system scripts refresh-from and cert-file (Scripts).]

Network Management and Monitoring

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

  [See Creating Action Scripts for YANG RPCs on Devices Running Junos OS and Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules.]

Known Limitations

There are no known limitations for vMX in Junos OS Release 21.2R1.

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 for vMX in Junos OS Release 21.2R1.

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

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

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

Resolved Issues: 21.2R1

IN THIS SECTION

Platform and Infrstarcture

- Traffic with jumbo frame might be discarded. PR1548422
- The AFT based line card might occasionally stops during start up, if the aftd-trio process gets multiple resync messages. The line card will then reboot. PR1567084

Documentation Updates

There are no errata and changes in Junos OS Release 21.2R1 for the vMX documentation.

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

Junos OS Release Notes for vRR

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 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

Learn about new features introduced in the Junos OS main and maintenance releases for vRR.

There are no new features for vRR in Junos OS Release 21.2R1.

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for vRR.

What's Changed in Release 21.2R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.2R1 for vRR.

Known Limitations

There are no known limitations for vRR in Junos OS Release 21.2R1.

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 21.2R1, see "Known Limitations" on page 140 for MX Series routers.

Open Issues

There are no known issues for vRR in Junos OS Release 21.2R1.

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 issues in Junos OS 21.2R1, see "Open Issues" on page 143 for MX Series routers.

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 21.2R1

IN THIS SECTION

To learn more about common BGP or routing resolved issues in Junos OS 21.2R1, see "Resolved Issues: 21.2R1" on page 164 for MX Series routers.

Platform and Infrastructure

- On the JRR200 devices, the option-60 vendor-class-identifier are not sent during ZTP. PR1582038

Documentation Updates

There are no errata and changes in Junos OS Release 21.2R1 for the vRR documentation.

Junos OS Release Notes for vSRX

IN THIS SECTION

These release notes accompany Junos OS Release 21.2R1 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

Learn about new features introduced in the Junos OS main and maintenance releases for vSRX.

Application Identification (AppID)

- **Multicast support in SD-WAN deployments (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX4100, SRX4200, SRX4600, vSRX)**—Starting in Junos OS Release 21.2R1, we've added support for multicast traffic on SRX Series devices in Provider Edge (PE) for SD-WAN deployments. The support for multicast traffic is available when the security device is operating with forwarding option set as flow-based.

  Support for multicast traffic results in bandwidth preservation and more efficient traffic flows.

  See [mode (Security Forwarding Options) and Virtual Routing and Forwarding Instances in SD-WAN Deployments].

- **SLA link preference enhancement (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, SLA link preference for security device interfaces supports custom link tags. You can define the link preferences using the `preferred-tag` and `affinity` options.

  This enhancement allows application traffic to switch from a lower-priority link to a higher-priority link that meets SLA requirements.

  [See Understanding Link-Type Affinity for the Preferred Link and sla-rule.]

- **Application-based load balancing support for APBR (NFX150, NFX250, NFX350, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)**—Starting in Junos OS Release 21.2R1, security devices support application-based load balancing for advanced policy-based routing (APBR). The APBR achieves load balancing by moving the application traffic in multiple WAN links using user-defined link selection criteria. The link selection criteria for application traffic depends on the link tag and link priority preference settings you defined for the advanced policy-based routing (APBR) interface. The application traffic distribution through the selected links depends on the link weight configuration.

  This feature improves the application traffic distribution performance for APBR and application quality of experience (AppQoE).

  [See Advanced Policy-Based Routing, sla-options, and interface.]

Flow-Based and Packet-Based Processing

- **Support for logging and session-close reasons (SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 HM, SRX1500, SRX4200, SRX4600, cSRX, and vSRX)**—Starting in Junos OS Release 21.2R1, we've enhanced the logging feature with support for the following flow functions:

  - Log for session-update
  - Support for 64-bit unified session-id
  - Adding new session close reason in session-close log

We've introduced a CLI command `log session-update` that you can use to update the session details.

[See Information Provided in Session Log Entries for SRX Series Services Gateways.]

Platform and Infrastructure

- **Mellanox support (vSRX 3.0)**—Starting in Junos OS Release 21.2R1, vSRX 3.0 instances that you deploy on VMware and kernel-based virtual machine (KVM) support the Mellanox ConnectX-4 and ConnectX-5 family adapters.

  [See vSRX Deployment for KVM.]

- **DPDK version upgrade (vSRX 3.0)**—Starting in Junos OS Release 21.2R1, we've upgraded the Data Plane Development Kit (DPDK) from version 18.11 to version 20.11. The new version supports ICE Poll Mode Driver (PMD), which enables the physical Intel E810 series 100G NIC support on vSRX 3.0. .

  In this release, Junos FreeBSD 12.X is vSRX 3.0 VM's guest OS. The Routing Engine and Packet Forwarding Engine run on Junos FreeBSD OS as one VM, and the Packet Forwarding Engine utilizes DPDK technologies such as DPDK ICE PMD and single-root I/O virtualization (SR-IOV).

  [See vSRX Deployment for KVM.]

Securing GTP and SCTP Traffic

- **Support for rate limiting based on APN-controlled aggregate rate limiting (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**–Starting in Junos OS Release 21.2R1, you can apply rate limiting for specific access point names (APNs) by using APN-controlled aggregate rate limiting (ARL). You can also configure APN groups and attach these groups to the GPRS tunneling protocol (GTP) profile for ARL. Configure the `apn-control` statement at the `[edit security gtp]` hierarchy level to enable the various configurations of APN-controlled ARL.

  [See profile (Security GTP), apn-control (Security GTP), apn-control-group (Security GTP), gtp, show security gtp profile, show security gtp counters, and show security gtp.]

VPNs

- **AutoVPN PSK support (SRX5000 line of devices with SPC3 card and vSRX running iked)**—To enable the VPN gateway to use a different IKE preshared key (PSK) for authenticating each remote peer, use the new CLI commands `seeded-pre-shared-key` *`ascii-text`* or `seeded-pre-shared-key` *`hexadecimal`* under the `[edit security ike policy` *`policy_name`*`]` hierarchy level. See policy.

  The SRX5000 line of devices with an SPC3 card and vSRX supports AutoVPN PSK only if the junos-ike-package is installed.

  To enable the VPN gateway to use the same IKE PSK for authenticating all remote peers, use the existing CLI commands `pre-shared-key` *`ascii-text`* or `pre-shared-key` *`hexadecimal`*.

We also introduce an optional configuration to bypass the IKE ID validation. Use the `general-ikeid` configuration statement under the `[edit security ike gateway gateway_name dynamic]` hierarchy level to bypass the IKE ID validation. If you enable this option, then during authentication of the remote peer, the SRX Series device and vSRX skips the IKE ID validation, and accepts all IKE ID types (hostname, user@hostname). See general-ikeid.

[See AutoVPN on Hub-and-Spoke Devices and Example: Configuring AutoVPN with Pre-Shared Key.]

- **Simplified packet drop identification for IPsec VPN services (SRX1500, SRX320, SRX340, SRX345, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 21.2R1, you can trace packet drop information without committing the configuration by using the `monitor security packet-drop` operational command for IPsec VPN services. This command includes various filters to generate the output fields according to your requirement.

  [See monitor security packet-drop.]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for vSRX.

What's Changed in Release 21.2R1

Junos XML API and Scripting

- **Changes to how command-line arguments are passed to Python op scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the device passes command-line arguments to a Python op script, it prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device prefixes a single hyphen (-) to all argument names.

  [See Declaring and Using Command-Line Arguments in Op Scripts.]

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you refresh a local commit, event, op, SNMP,

or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation.

When you refresh a script using the `request system scripts refresh-from` operational mode command, include the `cert-file` option and specify the certificate path. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See request system scripts refresh-from and cert-file (Scripts).]

Network Management and Monitoring

- **Changes to how command-line arguments are passed to Python action scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When a custom YANG RPC invokes a Python action script and passes command-line arguments to the script, the device prefixes a hyphen (-) to single-character argument names, and it prefixes two hyphens (--) to multi-character argument names. The prefix enables you to use standard command-line parsing libraries to handle the arguments. In earlier releases, the device passes the unmodified argument names to the script.

  [See Creating Action Scripts for YANG RPCs on Devices Running Junos OS and Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules.]

Known Limitations

Learn about known limitations in this release for vSRX.

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 SaaS DBs among all available links a best path chosen. If the link has no violation, and is the preferred link and has the highest priority among all live links, any further configuration change won't be recognized. The recommendation to the user is to configure all the preferences and priorities during configuration time so that all of it can be properly honored. PR1559662
- RPD core file is generated when the device reboots and process restarts. The process recovers and there is no service impact on routing protocol usage. PR1567043

- On vSRX3.0, the Layer 2 mode is not supported on SR-IOV interfaces. PR1584705

Open Issues

Learn about open issues in this release for vSRX.

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 downgraded to a release earlier than Junos OS Release 21.1 and then upgraded again to Junos OS Release 21.1, the application identification database tables might not get populated properly and have 0 entries. For such cases, after upgrading, uninstall and reinstall the signature package. PR1567199

J-Web

- If any VPN related configuration changes are done from the CLI and committed, click on the Monitor> Network > IPsec VPN menu to see the latest changes. PR1571751
- UI lists the IPsec VPNs information for uncommitted IPsec VPNs configuration under Monitor -> Netwrok -> IPsec VPN. PR1576609

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 21.2R1

IN THIS SECTION

Flow-Based and Packet-Based Processing

- The flowd or srxpfe process might crash when clearing the TCP proxy session. PR1573842

General Routing

- Packet drops might be seen with all commit events with 1G speed configured interface. PR1524614
- The Jflow version 5 functionality will not work correctly due to presence of new license infrastructure that is ported recently to vSRX3.0. PR1549988
- The pkid process runs at 100 percent when the device is unable to connect to a particular URL. PR1560374
- Fabric probe packets might be processed incorrectly when power-mode-ipsec is enabled. PR1564117
- The rpd process generates core files at boot time of a device. PR1567043
- The srxpfe process might stop and generate a core file during the feed update process. PR1579631
- When a vSRX was performing DNS sinkholing, the sinkhole response packets that it would generate had incorrect checksums. This would cause the receiving client to drop the packet and not be directed to the vSRX's sinkhole. PR1582827

Intrusion Detection and Prevention (IDP)

- On vSRX3.0 the attack-group-entries filters direction 0 limit 1 command is not showing expected values. PR1564761

- Application identification related signatures might not get triggered. PR1588450

J-Web

- J-Web GUI does not allow you to save a rule if the cumulative shared objects are more than 2500 before the policy grid is saved. When there are several shared objects, there will be a noticeable delay in opening sources and destinations of a rule, and performing the rule action. PR1540047
- After commit pending changes message is shown, the contents of other messages, landing page, or pop-ups are not visible completely. PR1554024
- To improve performance in Monitoring > Network > Interfaces page, the admin status is removed, services and protocols data merged into one host inbound traffic. PR1574895

Platform and Infrastructure

- COS queue egress interface forwarding-class might not work as expected. PR1538286
- If committing source-address <addr> routing-instance and than delete source-address <addr> in private edit mode, commit fails with warning message. PR1582529

Routing Protocols

- Traffic might be lost during mirror data transmit from the primary ppmd or bfdd. PR1570228

Documentation Updates

There are no errata and changes in Junos OS Release 21.2R1 for the vSRX documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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 21.2R1 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 21.2R1 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
        21.2K 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 21.2R1 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-x86-64-21.2-2020-06-06.0_RELEASE_21.2_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-
x86-64-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 21.2 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-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-21.2-2020-06-06.0_RELEASE_21.2_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-21.2-2020-06-06.0_RELEASE_21.2_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-21.2-2020-06-06.0_RELEASE_21.2_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-21.2-2020-06-06.0_RELEASE_21.2_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-21.2-2020-06-06.0_RELEASE_21.2_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-21.2-2020-06-06.0_RELEASE_21.2_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 21.2R1 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 21.2-2020-06-06.0_RELEASE_21.2_THROTTLE Kernel 64-bit
JNPR-11.0-20171012.170745_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: 21.2-2020-06-06.0_RELEASE_21.2_THROTTLE
JUNOS OS Kernel 64-bit  [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]
JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_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

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 19,4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.1.

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.

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.

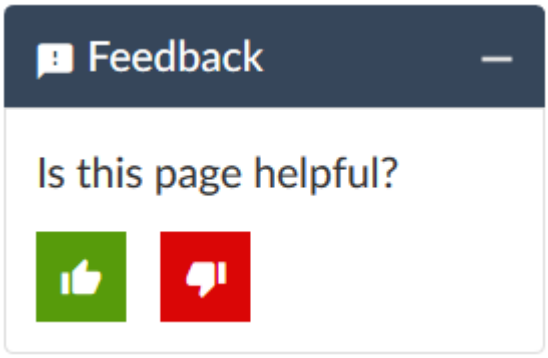
- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6.

  https://pathfinder.juniper.net/compliance/

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable)

Requesting Technical Support

IN THIS SECTION

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

29 July 2022—Revision 13, Junos OS Release 21.2R1– 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.

24 March 2022—Revision 12, Junos OS Release 21.2R1– 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.

22 February 2022—Revision 11, Junos OS Release 21.2R1– 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 October 2021—Revision 10, Junos OS Release 21.2R1– 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.

19 October 2021—Revision 9, Junos OS Release 21.2R1– 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.

7 October 2021—Revision 8, Junos OS Release 21.2R1– 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.

30 September 2021—Revision 7, Junos OS Release 21.2R1– 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 September 2021—Revision 6, Junos OS Release 21.2R1– 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.

26 August 2021—Revision 5, Junos OS Release 21.2R1– 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.

5 August 2021—Revision 4, Junos OS Release 21.2R1– QFX Series.

15 July 2021—Revision 3, Junos OS Release 21.2R1– 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.

8 July 2021—Revision 2, Junos OS Release 21.2R1– 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 June 2021—Revision 1, Junos OS Release 21.2R1– 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.