Release Notes

Published
2021-12-09

Junos ® OS 20.1R1 Release Notes

SUPPORTED ON

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

HARDWARE HIGHLIGHTS

- SRX380 Services Gateway and Software support for SRX380

SOFTWARE HIGHLIGHTS

- Sequential upgrade for Virtual Chassis (MX240, MX480, MX960, MX2010, MX2020, and MX10003)
- Delegation of IPv4 segment routing LSPs to a PCE (MX Series)
- gRPC Dial-Out support on JTI (ACX Series, MX Series, PTX Series, QFX Series)
- Unified ISSU with enhanced mode (MX240, MX480, MX960, MX2008, MX2010, MX2020)
- AppQoE support for granular APBR rules (SRX Series)
- Support for security policy reports (SRX Series)
- Support for UPN as User Identity (SRX Series)
- Trusted Platform Module (TPM) to bind secrets (SRX5400, SRX5600, and SRX5800)

IN FOCUS GUIDE

- Use this new guide to quickly learn about the most important Junos OS features and how you can deploy them in your network.

Release Notes: Junos® OS Release 20.1R1 for the ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, JRR Series, and Junos Fusion

10 December 2021

Contents

Introduction

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

These release notes accompany Junos OS Release 20.1R1 for the ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, JRR Series, and Junos Fusion. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

- **In Focus guide**—We have a document called In Focus that provides details on the most important features for the release in one place. We hope this document will quickly get you to the latest information about Junos OS features. Let us know if you find this information useful by sending an e-mail to techpubs-comments@juniper.net.
- **Important Information:**
  - Upgrading Using ISSU on page 231
  - Licensing on page 232
  - Compliance Advisor on page 232
  - Finding More Information on page 232
  - Documentation Feedback on page 233
  - Requesting Technical Support on page 234

Junos OS Release Notes for ACX Series

IN THIS SECTION

These release notes accompany Junos OS Release 20.1R1 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

Interfaces and Chassis

- **Support for new show | display set CLI commands (ACX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the following new **show** commands have been introduced:
  - **show | display set explicit**—Display explicitly, as a series of commands, all the configurations that the system internally creates when you configure certain statements from the top level of the hierarchy.
  - **show | display set relative explicit**—Display explicitly, as a series of commands, all the configurations that the system internally creates when you configure certain statements from the current hierarchy level.

[See show | display set and show | display set relative.]

Junos OS XML API and Scripting

- **The jcs:load-configuration template supports loading the rescue configuration (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the **jcs:load-configuration** template supports the **rescue** parameter to load and commit the rescue configuration on a device. SLAX and XSLT scripts can call the **jcs:load-configuration** template with the **rescue** parameter set to **"rescue"** to replace the active configuration with the rescue configuration.

  [See Changing the Configuration Using SLAX and XSLT Scripts and jcs:load-configuration Template.]

Junos Telemetry Interface

- **gRPC Dial-Out support on JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Junos OS Release 20.1R1 provides remote procedure call (gRPC) dial-out support for telemetry. In this method, the target device (server) initiates a gRPC session with the collector (client) and, when the session is established, streams the telemetry data that is specified by the sensor-group subscription to the collector. This is in contrast to the gRPC network management interface (gNMI) dial-in method, in which the collector initiates a connection to the target device.

  gRPC dial-out provides several benefits as compared to gRPC dial-in, including simplifying access to the target advice and reducing the exposure of target devices to threats outside of their topology.

  To enable export of statistics, include the **export-profile** and **sensor** statements at the [**edit services analytics**] hierarchy level. The export profile must include the reporting rate, the transport service (for example, gRPC), and the format (for example, gbp-gnmi). The sensor configuration should include the name of the collector (the server's name), the name of the export profile, and the resource path. An example of a resource path is **/interfaces/interface[name='fxp0'**.

  [See Using gRPC Dial-Out for Secure Telemetry Collection.]

- **gRPC version v1.18.0 with JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Junos OS Release 20.1R1 includes support for remote procedure call (gRPC) services version v1.18.0 with Junos telemetry interface (JTI). This version includes important enhancements for gRPC. In earlier releases, JTI is supported with gRPC version v1.3.0.

  Use gRPC in combination with JTI to stream statistics at configurable intervals from a device to an outside collector.

  [See gRPC Services for Junos Telemetry Interface.]

MPLS

- **CoS-based forwarding and policy-based routing to steer selective traffic over an SR-TE path (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 20.1R1, you can use CoS-based forwarding (CBF) and policy-based routing (PBR, also known as filter-based forwarding or FBF) to steer service traffic using a particular segment routing-traffic-engineered (SR-TE) path. This feature is supported only on uncolored segment routing LSPs that have the next hop configured as a first hop label or an IP address.

  With CBF and PBR, you can :

  - Choose an SR-TE path on the basis of service.
  - Choose the supporting services to resolve over the selected SR-TE path.

[See Example: Configuring CoS-Based Forwarding and Policy-Based Routing For SR-TE LSPs.]

Routing Protocols

- **Support for topology-independent loop-free alternate (TI-LFA) in IS-IS for IPv6-only networks (ACX Series, MX Series, and PTX Series)**— Starting with Junos OS Release 20.1R1, you can configure TI-LFA with segment routing in an IPv6-only network for the IS-IS protocol. TI-LFA provides MPLS fast reroute (FRR) backup paths corresponding to the post-convergence path for a given failure. TI-LFA provides protection against link failure, and node failure.

  You can enable TI-LFA for IS-IS by configuring the **use-post-convergence-lfa** statement at the **[edit protocols isis backup-spf-options]** hierarchy level. You can enable the creation of post-convergence backup paths for a given IPv6 interface by configuring the **post-convergence-lfa** statement at the **[edit protocols isis interface *interface-name* level *level*]** hierarchy level. The **post-convergence-lfa** statement enables link-protection mode.

  You can enable **node-protection** mode for a given interface at the **[edit protocols isis interface *interface-name* level *level* post-convergence-lfa]** hierarchy level. However, you cannot configure fate-sharing protection for IPv6-only networks.

  [See Understanding Topology-Independent Loop-Free Alternate with Segment Routing for IS-IS.]

System Management

- **Restrict option under NTP configuration is now visible (ACX Series, QFX Series, MX Series, PTX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the **noquery** command under the **restrict** hierarchy is now available and can be configured with a mask address. The **noquery** command is used to restrict ntpq and ntpdc queries coming from hosts and subnets.

  [See Configuring NTP Access Restrictions for a Specific Address.]

SEE ALSO

What's Changed

There are no changes in behavior and syntax for ACX Series in Junos OS Release 20.1R1.

SEE ALSO

- What's New | 14
- Known Limitations | 18
- Open Issues | 19
- Resolved Issues | 20
- Documentation Updates | 23
- Migration, Upgrade, and Downgrade Instructions | 23

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

- ACX6360 Junos telemetry interface or telemetry infrastructure does not support the interface-filtering capability. Therefore, after you enable a particular sensor for telemetry, it is turned on for all the interfaces. PR1371996
- ACX Series routers support only 900 joins of IGMPv3 users per second. PR1448146

SEE ALSO

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 ACX Series routers, which are acting as PE routers for Layer 2 VPN, Layer 2 circuit, VPLS, and Layer 3 VPN services, traffic forwarding over the MPLS paths used by these services can be stopped. you experience the traffic forwarding issue when the LSP flaps between the primary and the backup paths in a particular sequence. PR1204714
- The link fault signaling (LFS) feature is not supported on ACX5448 10-Gigabit, 40-Gigabit, and 100-Gigabit Ethernet interfaces. PR1401718
- When timing configuration and corresponding interface configurations are flapped for multiple times in iteration, PTP is stuck in **INITIALIZE** state where the ARP for the neighbor is not resolved. In the issue state, BCM hardware block gets into inconsistency state, where the lookup fails. PR1410746
- CoS table error might sometimes cause traffic outages and SNMP timeouts, if the optic module is plugged out and inserted back. PR1418696
- On ACX5000 platform, the high CPU usage by the fxpc process might be seen under a rare condition if parity errors are detected in devices. It has no direct service/traffic impact. However, because CPU utilization is high when this issue occurs, there are some side effects. For example, the issue could impact time-sensitive features such as BFD. PR1419761

- The configuration of em2 interface causes the FPC to crash during initialization and the FPC does not come online. To recover the FPC, first delete the em2 configuration, commit the configuration then restart the router. PR1429212
- Memory leaks are expected in Junos OS Release 20.1R1. PR1438358
- Recovery of Junos OS volume is not possible from the OAM menu. PR1446512
- On ACX500 and ACX4000, FFeb core could happen when heavy traffic of kernel trapped packets is received due to recent SDK upgrade for ACX devices. PR1465802
- - Issue seen during unified ISSU to Junos OS Releases 20.1- Unified ISSU will be completed, but the Packet Forwarding Engine will not function. - Impact will be forwarding will be affected. PR1483959

SEE ALSO

What's New | 14

What's Changed | 18

Known Limitations | 18

Resolved Issues | 20

Documentation Updates | 23

Migration, Upgrade, and Downgrade Instructions | 23

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.

General Routing

- On ACX5000 routers, the internal error **MacDrainTimeOut and bcm_port_update failed** is seen. PR1284590
- High CPU utilization is seen for fxpc processes with CoS changes on the aggregated Ethernet interfaces. PR1407098
- The optics module comes with Tx enabled by default. As the port is administratively disabled, the port is stopped but as the port has not been started, it does not disable Tx. PR1411015
- The l2cpd process might crash and generate a core file when interfaces flap. PR1431355
- ACX5448:DHCP packets are not transparent over Layer 2 circuit. PR1439518
- On the ACX5448, the flexible VLAN tagging encapsulation is not supported with MPLS family, need to provide commit ERROR. PR1445046
- Fans on an ACX5448-M might not be running at the correct speed. PR1448884
- The operating state for et- interfaces does not transit from init to normal. PR1449937
- ACX5448-D interfaces support: After the 100-Gigabit and 40-Gigabit Ethernet interface are disabled, the laser output power in the output of the **show interfaces diagnostics optics** command shows some values. PR1452323
- ACX5048 SNMP polling stops after the link is flapped or the SFP transceiver is replaced and **ACX_COS_HALP(acx_cos_gport_sched_set_strict_priority:987): Failed to detach** logs will be seen. PR1455722
- ACX5448-D and ACX5448-M devices do not display airflow information and temperature sensors as expected. PR1456593
- ACX5448 Layer 2 VPN with the **encapsulation-type ethernet** configuration, stops passing traffic after a random port is added with VLAN configuration. PR1456624
- The rpd might crash if a BGP route is resolved over the same prefix protocol next hop in the inet.3 table that has both RSVP and LDP routes. PR1458595
- Route resolution is not happening when the packet size is 10,000. PR1458744
- The traffic might be discarded silently during link recovery in an open ethernet access ring with ERPS configured. PR1459446
- ACX5000: SNMP MIB walk for jnxOperatingTemp is not returning anything for an FPC in new versions. PR1460391
- ACX5448-M interfaces and optics support: When you enable local loopback, the 10-Gigabit Ethernet interface goes down. PR1460715
- ACX5448-D interfaces and optics support: Sometimes when you bring up the aggregated Ethernet interface, there are ARP resolution issues. PR1461485

- On ACX Series platform, the LLDP neighbor is not up on the LAG after software upgrade to Junos OS Release 18.2R3-S1. PR1461831
- Not able to add more than 16 links in a LAG. PR1463253
- Memory leak on l2cpd process might lead to l2cpd crash. PR1469635
- RED drops are seen on interfaces even without any congestion. PR1470619
- The dcpfe core is seen when disabling or enabling MACsec through ACX6360-OR scripts. PR1479710
- ACX5448 Layer 2 VPN with interface ethernet-ccc input-vlan-map/output-vlan-map can cause trafficto be discarded silently. PR1485444

Interfaces and Chassis

- MC-AE interface might show unknown status if you add the subinterface as part of the VLAN on the peer MC-AE node. PR1479012

Layer 2 Ethernet Services

- Member links state might be asychronized on a connection between the PE and CE devices in an EVPN A/A scenario. PR1463791

Routing Protocols

- The rpd might crash continuously because of memory corruption in the IS-IS setup. PR1455432

SEE ALSO

What's New | **14**

What's Changed | **18**

Known Limitations | **18**

Open Issues | **19**

Documentation Updates | **23**

Migration, Upgrade, and Downgrade Instructions | **23**

Documentation Updates

IN THIS SECTION

This section lists the errata and changes in Junos OS Release 20.1R1 for the ACX Series documentation

Dynamic Host Configuration Protocol (DHCP)

- **Introducing DHCP User Guide**—Starting in Junos OS Release 20.1R1, we are introducing the DHCP User Guide for Junos OS routing, switching, and security platforms. This guide provides basic configuration details for your Junos OS device as DHCP Server, DHCP client, and DHCP relay agent.

  [See DHCP User Guide.]

SEE ALSO

- What's New | 14
- What's Changed | 18
- Known Limitations | 18
- Open Issues | 19
- Resolved Issues | 20
- Migration, Upgrade, and Downgrade Instructions | 23

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

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

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

SEE ALSO

- What's New | 14
- What's Changed | 18
- Known Limitations | 18
- Open Issues | 19
- Resolved Issues | 20
- Migration, Upgrade, and Downgrade Instructions | 23

Junos OS Release Notes for EX Series Switches

IN THIS SECTION

These release notes accompany Junos OS Release 20.1R1 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

NOTE: The following EX Series switches are supported in Release 20.1R1: EX2300, EX2300-C, EX3400, EX4300, EX4600-40F, EX4650, EX9200, EX9204, EX9208, EX9214, EX9251, and EX9253.

EVPN

- **Routing traffic between a VXLAN and a Layer 3 logical interface (EX4650 and QFX5120)—**Starting in Junos OS Release 20.1R1, EX4650 and QFX5120 switches support the routing of traffic between a Virtual Extensible LAN (VXLAN) and a Layer 3 logical interface. (You can configure the Layer 3 logical interface using the **set interfaces *interface-name* unit *logical-unit-number* family inet address *ip-address/prefix-length*** or the **set interfaces *interface-name* unit *logical-unit-number* family inet6 address *ipv6-address/prefix-length*** command.) This feature is enabled by default, so you do not need to take any action to enable it.

  > **NOTE:** By default, this feature is disabled on QFX5110 switches. To enable the feature on QFX5110 switches, you must perform the configuration described in Understanding How to Configure VXLANs and Layer 3 Logical Interfaces to Interoperate.

Interfaces and Chassis

- **Support for static link protection on aggregated interfaces (EX4650, QFX5120-32C, and QFX5120-48Y)**—Starting in Junos OS Release 20.1R1, you can enable link protection on aggregated interfaces for a specified static label-switched path (LSP). You can designate a primary and a backup physical link to support link protection. Egress traffic passes only through the designated primary link. This traffic includes transit traffic and locally generated traffic on the router. When the primary link fails, traffic is routed through the backup link.

  [See link-protection.]

Junos OS XML, API, and Scripting

- **The jcs:load-configuration template supports loading the rescue configuration (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the **jcs:load-configuration** template supports the **rescue** parameter to load and commit the rescue configuration on a device. SLAX and XSLT scripts can call the **jcs:load-configuration** template with the **rescue** parameter set to **"rescue"** to replace the active configuration with the rescue configuration.

  [See Changing the Configuration Using SLAX and XSLT Scripts and jcs:load-configuration Template.]

Junos Telemetry Interface

- **MPLS and local routing sensor streaming support on JTI (EX2300, EX3400, EX4300, EX4600, and EX9200)**—Junos OS Release 20.1R1 provides MPLS constrained-path Label Switched Paths (LSPs), RSVP-Traffic Engineering (RSVP-TE) and local routing statistics using Junos telemetry interface (JTI) and

remote procedure call (gRPC) services. Streaming statistics are sent to an outside collector at configurable intervals.

The following resource paths are supported:

- Local routing (resource path **/local-routes/**)
- MPLS constrained-path LSPs and RSVP-TE (resource path **/network-instances/network-instance/mpls/**)

To provision the sensor to export data through gRPC services, use the **telemetrySubscribe** RPC.

Streaming telemetry data through gRPC or gNMI also requires the OpenConfig for Junos OS module.

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

- **JTI infrastructure support for (EX2300, EX2300-MP, and EX3400)**—Junos OS Release 20.1R1 provides Junos telemetry interface (JTI) infrastructure support for EX2300, EX2300-MP, and EX3400 switches.

Layer 2 Features

- **Q-in-Q support on redundant trunk links using LAGs with link protection (EX4300-MP switches and Virtual Chassis)**—Starting in Junos OS Release 20.1R1, Q-in-Q is supported on redundant trunk links (also called "RTGs") using LAGs with link protection. Redundant trunk links provide a simple solution for network recovery when a trunk port on a switch goes down. In that case, traffic is routed to another trunk port, keeping network convergence time to a minimum.

  Q-in-Q support on redundant trunk links on a LAG with link protection also includes support for the following items:

  - Configuration of flexible VLAN tagging on the same LAG that supports the redundant links configurations
  - Multiple redundant links configurations on one physical interface
  - Multicast convergence

  [See Q-in-Q Support on Redundant Trunk Links Using LAGs with Link Protection.]

Multicast

- **PIM with IPv6 multicast traffic (EX4650 and QFX5120-48Y)**—Starting in Junos OS Release 20.1R1, EX4650 and QFX5120-48Y switches support Protocol Independent Multicast (PIM) with IPv6 multicast traffic as follows:

  - PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode (PIM-SDM)
  - PIM any-source multicast (PIM-ASM) and PIM source-specific multicast (PIM-SSM)
  - Static, embedded, and anycast rendezvous points (RPs)

[See PIM Overview.]

Routing Policy and Firewall Filters

- **Support for flexible-match-mask match condition (EX4650 and QFX-Series)**—Starting with Junos OS Release 20.1R1, for EX4650, QFX5120-32C, and QFX5120-48Y switches, the **flexible-match-mask** match condition in firewall filters is supported for the **inet**, **inet6**, and **ethernet-switching** families. With this feature, you can configure a filter by specifying the length of the match (4 bytes maximum) starting from a Layer 2 or Layer 3 packet offset.

  [See Firewall Filter Flexible Match Conditions.]

Storage and Fibre Channel

- **FIP snooping (EX4650-48Y and QFX5120-48Y)**—Starting in Junos OS Release 20.1R1, EX4650-48Y and QFX5120-48Y switches support Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) snooping. With FIP snooping enabled on these switches, you prevent unauthorized access and data transmission to a Fibre Channel (FC) network by permitting only those servers that have logged in to the FC network to access the network. You enable FIP snooping on FCoE VLANs when the switch is being used as an FCoE transit switch that connects FC initiators (servers) on the Ethernet network to FCoE forwarders at the FC storage area network (SAN) edge.

  [See Understanding FCoE Transit Switch Functionality and Understanding VN_Port to VN_Port FIP Snooping on an FCoE Transit Switch.]

System Management

- **Change status LED for network port to chassis beacon light (EX4300-48MP switch and EX4300-48MP Virtual Chassis)**—By default, when a network port and its associated link are active, the status LED for that port blinks green 8 times per second. Starting in Junos OS Release 20.1R1, you can use the **request chassis beacon** command to slow down the current blinking rate to 2 blinks per second. The slower-blinking and steadier green light acts as a beacon that leads you to an EX4300-48MP switch or a particular port in a busy lab.

  Using options with the **request chassis beacon** command, you can do the following for one or all network port status LEDs on a specified FPC:

  - Turn on the beacon light for:
    - 5 minutes (default)
    - A specified number of minutes (1 through 120)
  - Turn off the beacon light:
    - Immediately

- After a specified number of minutes (1 through 120)

After the beacon light is turned off, the blinking rate for the network port's status LED returns to 8 blinks per second.

[See request chassis beacon.]

Virtual Chassis

- **Virtual Chassis support for up to four member switches (EX4650)**—Starting in Junos OS Release 20.1R1, you can interconnect up to four EX4650-48Y switches into a Virtual Chassis managed as a single device. The Virtual Chassis:
  - Contains only EX4650-48Y switches.
  - Has two member switches in Routing Engine role (master, backup) and the remaining members in linecard role.
  - Supports 100GbE QSFP28 or 40GbE QSFP+ ports on the front panel (ports 48 through 55) as Virtual Chassis ports (VCPs).
  - Supports NSSU.

  A EX4650-48Y Virtual Chassis with two to four members now also supports the following protocol features that were not previously supported on a two-member EX4650-48Y Virtual Chassis:
  - IEEE 802.1X authentication
  - Layer 2 port security features, including IP source guard, IPv6 router advertisement (RA) guard, DHCP, and DHCP snooping
  - MPLS
  - Redundant trunk groups (RTG)

  EX4650-48Y Virtual Chassis has limitations on protocol feature support compared to the standalone switch. The following protocol features are not supported:
  - EVPN-VXLAN
  - Junos telemetry interface (JTI)
  - Multichassis link aggregation (MC-LAG)
  - Priority-based flow control (PFC)

  Configuration and operation are the same as for other EX Series and QFX Series Virtual Chassis.

[See Virtual Chassis Overview for Switches, 802.1X Authentication, MPLS Overview, DHCP Snooping, Understanding DHCP Snooping (ELS), Understanding IP Source Guard for Port Security on Switches, and Understanding IPv6 Router Advertisement Guard.]

SEE ALSO

What's Changed

IN THIS SECTION

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

Interfaces and Chassis

- **Logical Interface is created along with physical Interface by default (EX Series switches, QFX Series switches, MX Series routers)**—The logical interface is created on ge, et, xe interfaces along with the physical interface, by default. In earlier Junos OS Releases, by default, only physical interfaces were created. For example, for ge interfaces, earlier when you view the **show interfaces** command, by default, only the physical interface (ge-0/0/0), was displayed. Now, the logical interface (ge-0/0/0.16386) is also displayed.

Multicast

- **Multicast Layer 2 transit traffic statistics by multicast source and group (EX4600, EX4650, and the QFX5000 line of switches)**—Starting in Junos OS Release 20.1R1, EX4600, EX4650, and the QFX5000 line of switches provide statistics on the packet count for each multicast group and source when passing multicast transit traffic at Layer 2 with IGMP snooping. Run the **show multicast snooping route extensive** CLI command to see this count in the **Statistics: ... *n* packets** output field. The other statistics in that output field, **kBps** and **pps**, are not available (values displayed there are not valid statistics for multicast traffic at Layer 2). In earlier Junos OS releases, all three values in the **Statistics** output field for **kBps**, **pps**, and **packets** do not provide valid statistics for multicast traffic at Layer 2.

  [See show multicast snooping route.]

SEE ALSO

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for EX Series. For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Infrastructure

- If Junos OS panics with a file-system-related panic, such as 'dup alloc', recovery through the OAM shell might be needed. From the OAM shell, run 'fsck' on the root volume until it is marked clean. Only at this point, it is safe to reboot to the normal volume. PR1444941

Platform and Infrastructure

- The ge and mge ports have different color contrasts because of different vendors. PR1470312

SEE ALSO

What's New | 25

What's Changed | 31

Open Issues | 33

Resolved Issues | 36

Documentation Updates | 41

Migration, Upgrade, and Downgrade Instructions | 42

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 20.1R1 for EX Series. For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- On an EX9208 switch, a few xe- interfaces are going down with the error **if_msg_ifd_cmd_tlv_decode ifd xe-0/0/0 #190 down with ASIC Error**. PR1377840
- On EX2300 and EX4650 switches, unicast RPF check in strict mode might not work properly. PR1417546
- The time taken to install IPv4 or IPv6 routes into the FIB or delete them from the FIB is slowed down in Junos OS Release 19.3. Analysis shows that rpd learning rates are not degraded but RIB-to-FIB download rate is degraded. PR1441737
- On an EX9214 switch, if the MACsec-enabled link flaps after reboot, the error **errorlib_set_error_log(): err_id(-1718026239)** is observed. PR1448368
- In overall commit time, the evaluation of mustd constraints is taking 2 seconds more than usual. This is because the persist-group-inheritance feature has been made a default feature in the latest Junos OS releases. Eventually, this feature helps improve the subsequent commit times for scaled configurations significantly. The persist-group-inheritance feature is useful in customer scenarios where groups and nested groups are used extensively. In those scenarios, the group inheritance paths are not built every time, thus subsequent commits are faster. PR1457939
- On EX4300 switches, when packets entering a port exceed a size of 144 bytes, they might get dropped in very few cases. PR1464365
- Under certain conditions, FXPC core files might be generated when the Virtual Chassis reboots. Subsequently, the FXPC process comes up again and the Virtual Chassis is formed. PR1470185
- Memory issues are seen while you do NSSU from earlier Junos OS Release to Junos OS Release 20.1R1. Manually cleanup the space and run the **request system storage cleanup** command. PR1494963

Infrastructure

- On EX3400 and EX2300 switches, during zero-touch provisioning (ZTP) with configuration and image upgrade with file transfer through FTP, image upgrade is successful, but sometimes VM core files might be generated. PR1377721

Junos Fusion Provider Edge

- On a Junos fusion environment, intermediate traffic drop is seen between AD and SD when sFlow is enabled on an ingress interface. This issue is not seen always. When sFlow is enabled, the original packet gets corrupted for those packets that hit the sFlow filter. This is because a few packets transmitted from the egress interface of AD1 is short of FCS (4 bytes) + 2 bytes of data, due to which the drop occurs. It is seen that the normal data packets are of size 128 bytes (4 bytes FCS + 14 bytes Ethernet header + 20 bytes IP header + 90 bytes data), while the corrupted packet is 122 byte (14 bytes Ethernet header + 20 byte IP header + 88 bytes data). PR1450373

Junos Fusion Satellite Software

- In Junos fusion SP setup, EX4300 acting as satellite devices is generating temperature sensor alarm on multiple satellite devices modules connected to same aggregation device. PR1466324

Layer 2 Ethernet Services

- If **forward-only** is set within **dhcp-reply** in a Juniper Networks device as a DHCP relay agent, the DHCP DECLINE packets that are broadcasted from the DHCP client are dropped and not forwarded to the DHCP server. PR1429456

Multiprotocol Label Switching (MPLS)

- In case the two directly connected BGP peers are established over MPLS LSP, if the IP layer's MTU is smaller than the MPLS layer's MTU and the BGP packets from the host have the DF bit set, the BGP session might keep flapping because of the wrong TCP MSS in use. PR1493431

Platform and Infrastructure

- On EX9208 switches, traffic loss is observed if ingress and egress ports are in different FPCs. PR1429714
- On EX9208 switches, 33 percent degradation in MAC learning rate is seen in Junos OS Release 19.3R1 while comparing with Junos OS Release 18.4R1. PR1450729

Routing Protocols

- MUX state of the LACP interface sometimes does not change when **force-up** is configured. PR1484523
- During issue state, huge incorrect hold down value is displayed for the **show route table inet6** ***prefix*** **extensive** command. This is a display issue and actual hold down value is 120 seconds (This can be seen from RIPng traces) and routes are being deleted after 120 seconds. PR1493033

SEE ALSO

What's New | 25

What's New | 25

Known Limitations | 32

Resolved Issues | 36

Documentation Updates | 41

Migration, Upgrade, and Downgrade Instructions | 42

Resolved Issues

IN THIS SECTION

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

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

Authentication and Access Control

- On EX4600 and EX4300 switches, MAC entry is missing in the Ethernet switching table for Mac-radius client in server fail scenario when tagged is sent for two client. PR1462479

Class of Service (CoS)

- Shaping does not work after the reboot if **shaping-rate** is configured. PR1432078
- The traffic is placed in network-control queue on an extended port even if it comes in with different DSCP marking. PR1433252

EVPN

- The rpd might crash after the EVPN-related configuration is changed. PR1467309

Forwarding and Sampling

- Type 1 ESI/AD route might not be generated locally on the EVPN PE device in the **all-active** mode. PR1464778

General Routing

- The l2cpd process might crash and generate a core file when interfaces flap. PR1431355
- MicroBFD flap is seen when a QSFP transceiver is inserted into other port. PR1435221
- EX4600 Virtual Chassis does not come up after the Virtual Chassis port fiber connection is replaced with a DAC cable. PR1440062
- MAC addresses learned on an RTG might not be aged out after a Virtual Chassis member reboots. PR1440574
- Except one aggregated Ethernet member link, the other links do not send out sFlow sample packets for ingress traffic. PR1449568
- On EX3400 switches with half-duplex mode on 10-Mbps or 100-Mbps speed at medium traffic egress, traffic flow might stop on the port and MAC pause frames will be incrementing in the receive direction. PR1452209

- The l2ald and eventd processes are hogging 100 percent after the **clear ethernet-switching table** command is issued. PR1452738
- A firewall filter might not be applied in a particular Virtual Chassis or Virtual Chassis Fabric member as TCAM is running out of space. PR1455177
- Packet drop might be seen after removing and reinserting the SFP transceiver of the 40G uplink module ports. PR1456039
- Link-up delay and traffic drop might be seen on mixed SP L2/L3 and EP L2 type configurations. PR1456336
- The **syslog timeout connecting to peer database-replication** message is generated when the **show version detail** command is issued. PR1457284
- Overtemperature SNMP trap messages appear after an update even though the temperature is within the system thresholds. PR1457456
- The correct VoIP VLAN information in LLDP-MED packets might not be sent after commit if dynamic VoIP VLAN assignment is used. PR1458559
- The FXPC process might crash due to several BGP IPv6 session flaps. PR1459759
- On EX2300 and EX3400 switches, storage space limitation leads to image installation failure during phone home. PR1460087
- MAC addresses learned on redundant trunk group (RTG) might not be aged out after the aging time if the source interface is configured as RTG. PR1461293
- RTG link is down for nearly 20 seconds when the backup node is rebooting. PR1461554
- Configuring any combination of VLANs and interfaces under VSTP/MSTP might cause the VSTP/MSTP-related configuration to fail. PR1463251
- The Virtual Chassis function might be broken after an upgrade on EX2300 and EX3400 devices. PR1463635
- A few command lines to disable MAC learning are not working. PR1464797
- The jdhcpd might consume a high CPU and no further subscribers can be brought up if there are more than 4000 DHCP relay clients in the MAC move scenario. PR1465277
- On EX2300 switches, an FXPC core file is seen after mastership election based on the user's priority. PR1465526
- The broadcast and multicast traffic might be dropped over an IRB or a LAG interface in a Virtual Chassis scenario. PR1466423
- The MAC move message might have an incorrect **from** interface when MAC moves rapidly. PR1467459
- Optics measurements might not be streamed for interfaces of a PIC over JTI. PR1468435
- SSH session closes while you check the **show configuration | display set** command for both local and non-local users. PR1470695

- EX3400 switch is advertising only 100 Mbps when a speed of 100 Mbps is configured with autonegotiation enabled. PR1471931
- On EX4600 switches, the shaping of CoS does not work after reboot. PR1472223
- On EX3400 switches, CoS 802.1p bits rewrite might not happen in Q-in-Q mode. PR1472350
- The RIPv2 packets forwarded across a Layer 2 circuit connection might be dropped. PR1473685
- The dhcpd process might crash in a Junos fusion environment. PR1478375
- MX Series with MPCs/MICs based line-card might crash when there is a bulk route update failure in a corner case. PR1478392
- TFTP installation from loader prompt might not succeed on EX Series devices. PR1480348
- In an EVPN-VXLAN scenario, ARP request packets for an unknown host might be dropped in remote PE device. PR1480776

Infrastructure

- EX2300 switches might stop forwarding traffic or responding to the console. PR1442376
- On EX4300 switches, the CLI configuration **set chassis routing-engine on-disk-failure disk-failure-action (reboot | halt)** is not supported. PR1450093
- EX Series switches might not come up properly after reboot. PR1454950
- On EX4600 and EX4300 Virtual Chassis, error messages related to soft reset of port due to queue buffers being stuck could be seen. PR1462106
- Traffic is dropped on an EX4300-48MP device acting as a leaf device in a Layer 2 IP fabric EVPN-VXLAN environment. PR1463318
- EX3400 switches might reboot because of lack of watchdog patting. PR1469400
- In an EX2300 Virtual Chassis scenario, continuous dcpfe error messages and eventd process hog might be seen. PR1474808

Interfaces and Chassis

- VRRPv6 state is flapping with init and idle states after configuring **vlan-tagging**. PR1445370
- Traffic might be forwarded to incorrect interfaces in an MC-LAG scenario. PR1465077
- Executing commit might become unresponsive due to stuck device control process. PR1470622

Junos Fusion Enterprise

- Loop detection might not work on extended ports in Junos fusion scenarios. PR1460209

Junos Fusion Satellite Software

- In Junos fusion for enterprise, the dpd crash might be observed on satellite devices running SNOS. PR1460607

Layer 2 Features

- MAC or ARP learning might not work for copper base SFP-T transceivers on EX4600 switches. PR1437577
- The Link Layer Discovery Protocol (LLDP) function might fail when a Juniper device connects to a non-Juniper device. PR1462171
- After rebooting, an FXPC core file might be seen when committing the configuration. PR1467763
- Traffic might be affected if composite next-hop is enabled. PR1474142

Layer 2 Ethernet Services

- Member links state might be asynchronized on a connection between PE and CE devices in an EVPN A/A scenario. PR1463791

Platform and Infrastructure

- NSSU causes traffic loss again after the backup to master transitions. PR1448607
- In a Virtual Chassis scenario, the IRB traffic might get dropped after master switchover. PR1453025
- The OSPF neighbor might go down when mDNS/PTP traffic is received at a rate higher than 1400 pps. PR1459210
- ERP might not revert to IDLE state after reload or reboot of multiple switches. PR1461434
- On EX4300 Virtual Chassis, traffic loss might be observed longer than 20 seconds when performing NSSU. PR1461983
- On EX2300 and EX3400 switches, the upgrade might fail as there is not enough space. PR1464808
- On EX4300 switches, IGMP reports are dropped when mixed enterprise and service provider configuration styles are used. PR1466075

- On EX4300 switches, an input firewall filter attached to isolated or community VLANs fails to match dot1p bits on the VLAN header. PR1478240
- Virtual Chassis VRRP peer drops packets destined to the VRRP VIP after IRB is disabled. PR1491348

Routing Protocols

- Host-destined packets with the filter log action might not reach the Routing Engine if log or syslog is enabled. PR1379718
- On EX9208 platforms, BGP IPv4 or IPv6 convergence and RIB install or delete time are degraded in Junos OS Releases 19.1R1, 19.2R1, 19.3R1, and 19.4R1. PR1414121
- The **other querier present interval** timer cannot be changed in an IGMP/MLD snooping scenario. PR1461590

User Interface and Configuration

- Problem with access to J-Web after updating from Junos OS Release 18.2R2 to Release 18.2R3. PR1454150
- Error message **umount: unmount of /.mount/var/val/chroot/packages/mnt/jweb-ex32-d2cf6f6b failed: Device busy** is seen when Junos OS is upgraded with the **validate** option. PR1478291

SEE ALSO

What's New | 25

What's Changed | 31

Known Limitations | 32

Open Issues | 33

Documentation Updates | 41

Migration, Upgrade, and Downgrade Instructions | 42

Documentation Updates

IN THIS SECTION

- Dynamic Host Configuration Protocol (DHCP) | 42

This section lists the errata and changes in Junos OS Release 20.1R1 documentation for the EX Series.

Dynamic Host Configuration Protocol (DHCP)

- **Introducing DHCP User Guide**—Starting in Junos OS Release 20.1R1, we are introducing the DHCP User Guide for Junos OS routing, switching, and security platforms. This guide provides basic configuration details for your Junos OS device as DHCP Server, DHCP client, and DHCP relay agent.

  [See DHCP User Guide.]

SEE ALSO

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

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

SEE ALSO

- What's New | 25
- What's Changed | 31
- Known Limitations | 32
- Open Issues | 33
- Resolved Issues | 36
- Documentation Updates | 41

Junos OS Release Notes for JRR Series

IN THIS SECTION

These release notes accompany Junos OS Release 20.1R1 for JRR Series. They describe new and changed features, limitations, and known and resolved problems in the hardware.

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

What's New

There are no new features or enhancements to existing features for JRR Series in Junos OS Release 20.1R1.

SEE ALSO

- What's Changed | 44
- Known Limitations | 45
- Open Issues | 45
- Resolved Issues | 46
- Documentation Updates | 46
- Migration, Upgrade, and Downgrade Instructions | 47

What's Changed

There are no changes in behavior and syntax for JRR Series in Junos OS Release 20.1R1.

SEE ALSO

- What's New | 44
- Known Limitations | 45
- Open Issues | 45
- Resolved Issues | 46
- Documentation Updates | 46
- Migration, Upgrade, and Downgrade Instructions | 47

Known Limitations

There are no known limitations for JRR Series in Junos OS Release 20.1R1.

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

SEE ALSO

- What's New | 44
- What's Changed | 44
- Open Issues | 45
- Resolved Issues | 46
- Documentation Updates | 46
- Migration, Upgrade, and Downgrade Instructions | 47

Open Issues

There are no open issues for JRR Series in Junos OS 20.1R1 Release.

SEE ALSO

- What's New | 44
- What's Changed | 44
- Known Limitations | 45
- Resolved Issues | 46
- Documentation Updates | 46
- Migration, Upgrade, and Downgrade Instructions | 47

Resolved Issues

IN THIS SECTION

Learn about resolved issues for JRR Series in Junos OS 20.1R1 Release.

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

General Routing

- JRR200: USB install image is not working. PR1471986

SEE ALSO

- What's New | 44
- What's Changed | 44
- Known Limitations | 45
- Open Issues | 45
- Documentation Updates | 46
- Migration, Upgrade, and Downgrade Instructions | 47

Documentation Updates

There are no errata or changes in Junos OS Release 20.1R1 documentation for JRR200 Route Reflectors.

SEE ALSO

- What's New | 44
- What's Changed | 44

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 Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

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

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

SEE ALSO

Junos OS Release Notes for Junos Fusion Enterprise

IN THIS SECTION

These release notes accompany Junos OS Release 20.1R1 for Junos Fusion Enterprise. Junos Fusion Enterprise is a Junos Fusion that uses EX9200 switches in the aggregation device role. These release notes describe new and changed features, limitations, and known problems in the hardware and software.

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

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

What's New

There are no new features or enhancements to existing features in Junos OS Release 20.1R1 for Junos fusion for enterprise.

> **NOTE:** For more information about the Junos fusion for enterprise features, see the Junos fusion for enterprise User Guide.

SEE ALSO

- What's Changed | 49
- Known Limitations | 50
- Open Issues | 50
- Resolved Issues | 51
- Documentation Updates | 52
- Migration, Upgrade, and Downgrade Instructions | 52

What's Changed

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 20.1R1 for Junos fusion for enterprise.

SEE ALSO

- What's New | 49
- Known Limitations | 50
- Open Issues | 50
- Resolved Issues | 51
- Documentation Updates | 52
- Migration, Upgrade, and Downgrade Instructions | 52

Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 20.1R1 for Junos fusion for enterprise.

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

SEE ALSO

Open Issues

IN THIS SECTION

This section lists the known issues in hardware and software in Junos OS Release 20.1R1 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.

Junos Fusion for Enterprise

- In a Junos fusion, intermediate traffic drop might be seen between the aggregation and satellite device when sFlow is enabled on the ingress interface. When sFlow is enabled, the original packet is corrupted for those packets that hit the sFlow filter. This is because the packets exiting the aggregation device are short of 4 bytes of FCS and 2 bytes of data. Normal data packets are 128 bytes (4 bytes for FCS, 14

bytes for Ethernet header, 20 bytes for IP header, and 90 bytes for data). The corrupted packets are 122 bytes (14 bytes for Ethernet header, 20 bytes for IP header, and 88 bytes for data). PR1450373

- In a Junos fusion, an EX4300 acting as the satellite device is triggering the temperature sensor alarm on multiple satellite device modules connected to same aggregation device. PR1466324

SEE ALSO

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: 20.1R1

- Loop detection might not work on extended ports in a Junos fusion for enterprise scenario. PR1460209
- The dpd process might generate a core file on satellite devices in Junos fusion for enterprise. PR1460607

SEE ALSO

Documentation Updates

There are no errata or changes in Junos OS Release 20.1R1 for documentation for Junos fusion for enterprise.

SEE ALSO

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/junos-install-ex92xx-x86-64-18.3B1.n.tgz
```

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

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

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

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

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

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

Rebooting occurs only if the upgrade is successful.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

Preparing the Switch for Satellite Device Conversion

There are multiple methods to upgrade or downgrade satellite software in your Junos fusion 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 17.1, 17.2, and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

Downgrading from Junos OS

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

SEE ALSO

- What's New | 49
- What's Changed | 49
- Known Limitations | 50
- Open Issues | 50
- Resolved Issues | 51
- Documentation Updates | 52

Junos OS Release Notes for Junos Fusion Provider Edge

IN THIS SECTION

These release notes accompany Junos OS Release 20.1R1 for the Junos Fusion Provider Edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

Learn about new features introduced in this release for Junos fusion Provider Edge routers.

Hardware

- **Support for MX10008 and MX10016**—Starting in Junos OS Release 20.1R1, Junos fusion for provider edge supports the use of an MX10008 or MX10016 router as an aggregation device which acts as the single point of management for all devices in the Junos fusion.

  [See Understanding Junos Fusion Provider Edge Software and Hardware Requirements.]

SEE ALSO

What's Changed

There are no changes in the behavior of Junos OS features or in the syntax of Junos OS statements and commands in this release for Junos fusion for provider edge.

SEE ALSO

Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 20.1R1 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.

SEE ALSO

Open Issues

IN THIS SECTION

Learn about open issues in this release 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.

Junos Fusion Provider Edge

- On a Junos fusion system, intermediate traffic drop might be seen between the aggregation and satellite device when SFlow is enabled on the ingress interface. When SFlow is enabled, the original packet is corrupted for those packets that hit the SFlow filter. This is because the packets egressing the aggregation device are short of 4 bytes of FCS 2 bytes of data. Normal data packets are 128 bytes (4 bytes for FCS, 14 bytes for Ethernet header, 20 bytes for IP header and 90 bytes for data). The corrupted packets are 122 bytes (14 bytes for Ethernet header, 20 bytes for IP header, and 88 bytes for data).PR1450373

SEE ALSO

- What's New | 58
- What's Changed | 59
- Known Limitations | 60
- Resolved Issues | 61
- Documentation Updates | 62
- Migration, Upgrade, and Downgrade Instructions | 62

Resolved Issues

There are no fixed issues in the Junos OS Release 20.1R1 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.

SEE ALSO

- What's New | 58
- What's Changed | 59
- Known Limitations | 60
- Open Issues | 60
- Documentation Updates | 62
- Migration, Upgrade, and Downgrade Instructions | 62

Documentation Updates

There are no errata or changes in Junos OS Release 20.1R1 documentation for Junos fusion for provider edge.

SEE ALSO

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 20.1R1 is different from that for earlier Junos OS releases.

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

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

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

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

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

5. Select the **Software** tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

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

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

- For 64-bit software:

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

```
user@host> request system software add validate reboot
source/jinstall64-20.1R1.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot
source/jinstall-20.1R1.SPIN-domestic-signed.tgz
```

All other customers, use the following commands.

- For 64-bit software:

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

```
user@host> request system software add validate reboot
source/jinstall64-20.1R1.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot
source/jinstall-20.1R1.SPIN-export-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

> **NOTE:** After you install a Junos OS Release 20.1R1 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

Preparing the Switch for Satellite Device Conversion

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

> **NOTE:** The following conditions must be met before a standalone switch that is running Junos OS Release 14.1X53-D43 can be converted to a satellite device when the action is initiated from the aggregation device:
>
> - The switch can be converted to only SNOS 3.1 and later.
> - Either the switch must be set to factory-default configuration by using the **request system zeroize** command, or the following command must be included in the configuration: **set chassis auto-satellite-conversion**.

Customers with EX4300 switches, use the following command:

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

Customers with QFX5100 switches, use the following command:

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

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

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

2. Clear the device:

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

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

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

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

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

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

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

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

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

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, and preconfiguration. See Configuring Junos fusion 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 20.1R1, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

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

Downgrading from Junos OS Release 20.1

To downgrade from Release 20.1 to another supported release, follow the procedure for upgrading, but replace the 20.1 **jinstall** package with one that corresponds to the appropriate release.

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

For more information, see the Installation and Upgrade Guide.

SEE ALSO

- What's New | 58
- What's Changed | 59
- Known Limitations | 60
- Open Issues | 60
- Resolved Issues | 61
- Documentation Updates | 62

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

IN THIS SECTION

These release notes accompany Junos OS Release 20.1R1 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

Learn about new features introduced in Junos OS Release 20.1R1 for MX Series routers.

Hardware

NOTE: The MX2K-MPC11E line card is supported in Junos OS 19.3R2 and later 19.3 releases and in Junos OS 20.1R1 and later Junos OS releases. It is not supported in any Junos OS 19.4 releases.

Class Of Service

- **Hierarchical CoS support on MX2K-MPC11E line cards (MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 20.1R1, hierarchical CoS is supported on MX2K-MPC11E line cards.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Protocols and Applications Supported by the MX2K-MPC11E.]

- **Forwarding CoS (L2 classifiers, rewrite) support on MX2K-MPC11E line cards (MX2008, MX2010, and MX2020)**—Starting in Release 20.1R1, Junos OS supports forwarding CoS (L2 classifiers, rewrite) for MX Series routers with MX2K-MPC11E line cards.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Protocols and Applications Supported by the MX2K-MPC11E.]

- **Seamless MPLS CoS support for pseudowires from access node and multiservices edge (MSE) node on MX2K-MPC11E line cards (MX2008, MX2010, and MX2020)**—Starting with Junos OS Release 20.1R1, we support on the MX2K-MPC11E line card pseudowires from access node and multiservices edge (MSE) node for MX2008, MX2010, and MX2020 routers to include seamless MPLS CoS (BA and MF classifiers, rewrite rules, schedulers, drop profiles, policers, HQoS support — interface-set, physical interface level, S-VLAN level, logical unit/C-VLAN level, and traffic-control profile).

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Protocols and Applications Supported by the MX2K-MPC11E.]

- **CoS support for forwarding class counters on MX2K-MPC11E line cards (MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 20.1R1, we support forwarding class counters on MX2K-MPC11E line cards. This feature was originally introduced in Junos OS Release 14.1.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

[See Protocols and Applications Supported by the MX2K-MPC11E.]

- **Layer 2.5 injection of control traffic to ensure queuing on GRE tunnel with CoS settings intact (MX204 and devices installed with next-generation MPCs (MPC2E-NG and MPC3E-NG))**—Starting with Junos OS Release 20.1R1, you can configure host-injected control traffic to reache the GRE tunnel interface queues at the packet forwarding engine when the control session is over the GRE tunnel interface. This includes control protocols OSPF, BGP, PIM, RSVP, LDP, OAM, BFD, and MSDP. Injection of control traffic ensures that the kernel includes the interface ID of the GRE logical interface and the unicast next-hop ID of the corresponding GRE physical interface along with the packet that is injected into the packet forwarding engine.

  With this feature enabled, all transit packets on the GRE tunnel logical interface have the ToS copied to the outer header. To enable this feature, configure the **force-control-packets-on-transit-path** statement on the GRE tunnel logical interface.

  [See force-control-packets-on-transit-path.]

EVPN

- **Support for EVPN functionality on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS 20.1R1, you can configure MX2K-MPC11E line cards on MX2010 and MX2020 routers to support single-homed devices on an EVPN-MPLS network.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See EVPN Multihoming Overview.]

Forwarding and Sampling

- **Support for load balancing on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, the following advanced Layer 2 features are supported on MX2010 and MX2020 routers with MX2K-MPC11E line cards and Enhanced Switch Fabric Boards (SFB3s): enhanced hash-key options, consistent flow hashing, symmetrical load balancing over 802.3ad LAGs, source IP only hashing, and destination IP only hashing.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Configuring Per-Flow Load Balancing Based on Hash Values.]

General Routing

- **Support for GRE key (MX Series)**—Starting with Junos OS 20.1R1, Junos OS supports configuring a key to identify traffic flows in a GRE tunnel as defined in RFC2890. You must configure the key on the routers on both endpoints of a tunnel and create an export policy to populate the key in the forwarding table. You can configure **dynamic-tunnel-gre-key** at the **[edit routing-options dynamic-tunnels tunnel-attributes *name*]** hierarchy level.

  [See dynamic-tunnel-gre-key.]

High Availability and Resiliency

- **Unified ISSU with enhanced mode (MX240, MX480, MX960, MX2008, MX2010, MX2020)**—Starting in Junos OS Release 20.1R1, MX Series routers with MPC8E, or MPC9E line cards installed can use a new ISSU option called *enhanced mode*. Enhanced mode eliminates packet loss during the unified ISSU

process by running a copy of the Junos OS software in standby mode ready to take over when software moves from an old image to a new one.

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

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

- **Sequential upgrade for Virtual Chassis (MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 20.1R1, MX Series Virtual Chassis configurations can use sequential upgrade to install new software releases with minimal network downtime. Sequential upgrade is an alternative to unified ISSU that installs a new release and reboots each Virtual Chassis member router one at a time. While the upgrade happens on one member router, the other member router continues to operate and handle network operations.

  To perform a sequential upgrade in an MX Series Virtual Chassis, you first issue the **request virtual-chassis upgrade protocol-backup *package-name*** command from the CLI for the Virtual Chassis master router. This initiates the upgrade process on the Virtual Chassis backup router. After the upgrade finishes on the backup router, issue the **request virtual-chassis upgrade protocol-master *package-name*** command from the backup router CLI to begin the same upgrade process for the Virtual Chassis master router.

  [See How to Use Sequential Upgrade in an MX Series Virtual Chassis.]

- **Support for BFD on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, MX2010 and MX2020 routers with the MX2K-MPC11E line card support the following BFD features:

  - Centralized BFD
  - Distributed BFD
  - Inline BFD (single-hop only)
  - Single-hop BFD
  - Multihop BFD
  - Micro BFD
  - BFD over IRB interfaces
  - BFD over pseudowire over logical tunnel and redundant logical tunnel interfaces
  - Virtual circuit connectivity verification (VCCV) BFD for Layer 2 VPNs, Layer 2 circuits, and virtual private LAN service (VPLS)

  Micro BFD at the Packet Forwarding Engine level behaves slightly differently on MX2K-MPC11E line cards. If micro BFD is enabled on an aggregated Ethernet (ae) interface, the micro BFD packets are not subjected to firewall filters for both tagged and untagged ae interfaces.

> **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

[See Understanding BFD for Static Routes for Faster Network Failure Detection and Understanding Distributed BFD.]

Interfaces and Chassis

- **Support for flexible tunnel interfaces (MX240, MX480, and MX960 with MPC10E; MX2010 and MX2020 with MPC11E)**—Starting in Junos OS Release 20.1R1, MX Series routers with MPC10E or MPC11E line cards support flexible tunnel interfaces (FTIs). FTIs support Layer 3 point-to-point tunnels, which use Virtual Extensible LAN (VXLAN) encapsulation with a Layer 2 pseudo header.

  To configure FTIs on your device and to enable multiple encapsulations on the FTIs, use the **vxlan-gpe** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* tunnel encapsulation]** hierarchy level.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Flexible Tunnel Interfaces Overview and vxlan-gpe (FTI).]

- **Support for ALB on multiple Packet Forwarding Engines for aggregated Ethernet bundles (MX Series MPCs)**—Starting in Junos OS Release 20.1R1, on MX Series MPCs, adaptive load balancing (ALB) for aggregated Ethernet bundles evenly redistributes the traffic load across multiple ingress Packet Forwarding Engines on the same line card, thus providing flexibility and redundancy. In earlier releases, ALB evenly redistributes traffic across all ingress traffic on a single Packet Forwarding Engine only. ALB is disabled by default.

  > **NOTE:** MPC3E does not support adaptive load balancing.

  To configure ALB, include the **adaptive** statement at the [**edit interfaces ae-interface aggregated-ether-options load-balance**] hierarchy level.

> **NOTE:** When you configure locality bias and adaptive load balancing for aggregated Ethernet interfaces, ALB is supported per Packet Forwarding Engine and not across all Packet Forwarding Engines on the same line card. Also, you cannot revert to ALB support per Packet Forwarding Engine after you enable ALB support on multiple Packet Forwarding Engines.

[See Configuring Adaptive Load Balancing.]

- **Adaptive load balancing on MPC10E-15C-MRATE, MPC10E-10C-MRATE, and MX2K-MPC11E line cards (MX240, MX480, MX960, and MX2020)**—Starting in Junos OS Release 20.1R1, adaptive load balancing (ALB) is supported on aggregated Ethernet bundles and ECMP links to correct traffic imbalance among member links. ALB resolves traffic load imbalance caused by the hashing algorithm. With ALB configured on the system, traffic is balanced across member links when an imbalance is detected.
  - To configure ALB on aggregated Ethernet bundles, run the **set interfaces name aggregated-ether-options load-balance adaptive tolerance** command. [See adaptive.]
  - To configure ALB on ECMP links, run the **set chassis ecmp-alb tolerance** command. [See ecmp-alb.]

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Example: Configuring Aggregated Ethernet Load Balancing.]

- **VLAN TCC encapsulation on aggregated Ethernet interfaces (MX Series)**—Starting in Junos OS Release 20.1R1, aggregated Ethernet interfaces support VLAN translational cross-connect (TCC) encapsulation. For configuring VLAN TCC encapsulation, you must have the member links of aggregated Ethernet with VLAN TCC encapsulation supported hardware.

  > **NOTE:** MX Series routers do not perform any external commit check for member links of aggregated interfaces for the VLAN TCC encapsulation supported hardware.

  - Enable the **extended-vlan-tcc** option for aggregated Ethernet interfaces at the **[edit interfaces *interface-name* encapsulation]** hierarchy level to configure extended 802.1q tagging for TCC.
  - Enable the **vlan-tcc** option for aggregated Ethernet interfaces at the **[edit interfaces *interface-name* unit logical-unit-number encapsulation]** hierarchy level to configure 802.1q tagging for TCC.
  - Enable the **inet-address** option for aggregated Ethernet interfaces at the **[edit interfaces *interface-name* unit logical-unit-number family tcc proxy]** hierarchy level to configure proxy host address on the non-Ethernet side of Ethernet TCC circuits.

- Enable the **inet-address** option for aggregated Ethernet interfaces at the **[edit interfaces *interface-name* unit logical-unit-number family tcc remote]** hierarchy level to configure remote host address on the non-Ethernet side of Ethernet TCC circuits.
- Enable the **mac-address** option for aggregated Ethernet interfaces at the **[edit interfaces *interface-name* unit logical-unit-number family tcc remote]** hierarchy level to configure remote MAC address on the non-Ethernet side of Ethernet TCC circuits.
- Enable the **tcc** option for aggregated Ethernet interfaces at the **[edit interfaces *interface-name* unit logical-unit-number family]** hierarchy level to configure the TCC protocol suite.

[See Configuring VLAN TCC Encapsulation.]

- **MX2K-MPC11E supports Junos node slicing (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, the MX2K-MPC11E supports Junos node slicing and abstracted fabric (af) interfaces. Using Junos node slicing, you can create multiple partitions in a single physical MX Series router. Each partition, referred to as a guest network function (GNF), behaves as an independent router. An af interface is a pseudointerface that exhibits a first-class Ethernet interface behavior. The af interface facilitates routing control and management traffic between GNFs through the switch fabric. In a Junos node slicing deployment, the MX2K-MPC11E interoperates with all MPCs that support the af interfaces.

  NOTE:
  - The MX2K-MPC11E interoperates only with the Switch Fabric Board SFB3.
  - The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Understanding Junos Node Slicing.]

- **Support for rate selectability on MX2K-MPC11E line cards (MX2010 and MX2020)**—In Junos OS Releases 19.3R2 and 20.1R1, we introduce a new fixed-configuration, rate-selectable line card, MX2K-MPC11E. The line-card has 40 built-in ports that can operate at 100-Gbps speed. You can configure all ports in a PIC to operate at the same speed or configure all the ports at different supported speeds. With QSFP28 optics installed, all ports operate at a default speed of 100-Gbps. In addition, you can use QSFP+ optics on Port 0 of every PIC and configure it as:
  - A 40-Gbps interface
  - Four 10-Gbps interfaces (channels), using breakout cables

  NOTE: The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Introduction to Rate Selectability.]

- **Distributed LACP support in PPM AFT on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, the MX2K-MPC11E line card supports distributed LACP. Distributed LACP support is managed by the advanced forwarding toolkit (AFT)-based periodic packet manager (PPMAN). In earlier releases, and for other line cards except MPC10E, distributed LACP support is managed by the Junos OS-based PPMAN.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Periodic Packet Management.]

- **Optimize fabric path to prevent traffic hop with MX2K-MPC11E line cards (MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 20.1R1, on MX2008, MX2010, and MX2020 routers with MX2K-MPC11E, you can optimize the fabric path of the traffic flowing over abstracted fabric (af) interfaces between two guest network functions (GNFs) by configuring fabric optimization mode. This feature reduces fabric bandwidth consumption by preventing any additional fabric hop (switching of traffic flows from one Packet Forwarding Engine to another because of load balancing on the af interface) before the packets eventually reach the destination Packet Forwarding Engine.

  To configure fabric optimization mode, use the following CLI command at the base system (BSYS): **set chassis network-slices guest-network-functions gnf *id* collapsed-forward (monitor | optimize)**.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Optimizing Fabric Path for Abstracted Fabric Interface.]

- **Chassis and power management for MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, the MX2010 and MX2020 routers with the MX2K-MPC11E line card support chassis management features, including field- replaceable unit (FRU) management, power budgeting and management, and environmental monitoring.

  The MX2K-MPC11E line card supports the following configuration:

  - The ambient temperature is less than 46°C.
  - The ports on the MX2K-MPC11E line cards operate at various modes or speeds (10-Gbps, 40-Gbps, or 100 Gbps). The pic-mode specifies the speed of the active ports. If pic-mode is not specified, then the default mode is 100 Gbps.
  - Supports dynamic power management.
  - Supports both hyper mode (the default mode) and normal mode.

- Supports both normal mode (the deafult mode) and enhanced priority mode for interface schedulers.
- Supports interface queueing modes, namely WAN port queueing mode (the default mode), limited queueing mode, and enhanced queueing mode.

> **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

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

- **MPC Protocol and Application Support for MX2K-MPC11E line cards**—Starting in 20.1R1, MX2020 and MX2010 routers with MX2K-MPC11E line cards support many MPC protocols and applications. For a complete list, see *Protocols and Applications Supported by the MX2K-MPC11E*.
  - Standard Generic Routing Encapsulation (GRE)
  - Bidirectional Forwarding Detection protocol (BFD)
  - Internet Control Message Protocol (ICMP) and ICMPv6
  - Border Gateway Protocol (BGP)
  - BGP/MPLS virtual private networks (VPNs)
  - Logical system and Virtual routing and forwarding (VRF) routing instances
  - Load Balancing
  - Class of Service (CoS)—per port, virtual LAN (VLAN), Point-to-Point Protocol over Ethernet (PPPoE) or Dynamic Host Configuration Protocol (DHCP), Egress hierarchical class-of-service (CoS) shaping
  - Layer 2 Features
  - Firewall filters and policers

> **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

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

- **Support for new show | display set CLI commands (ACX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the following new **show** commands have been introduced:
  - **show | display set explicit**—Display explicitly, as a series of commands, all the configurations that the system internally creates when you configure certain statements from the top level of the hierarchy.

- **show | display set relative explicit**—Display explicitly, as a series of commands, all the configurations that the system internally creates when you configure certain statements from the current hierarchy level.

[See show | display set and show | display set relative.]

Junos OS, XML, API, and Scripting

- **The jcs:load-configuration template supports loading the rescue configuration (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the **jcs:load-configuration** template supports the **rescue** parameter to load and commit the rescue configuration on a device. SLAX and XSLT scripts can call the **jcs:load-configuration** template with the **rescue** parameter set to **"rescue"** to replace the active configuration with the rescue configuration.

  [See Changing the Configuration Using SLAX and XSLT Scripts and jcs:load-configuration Template.]

Junos Telemetry Interface

- **IS-IS adjacency and LSDB event streaming support on JTI (MX960, PTX1000, and PTX10000)**—Junos OS Release 20.1R1 provides IS-IS adjacency and link-state database (LSDB) statistics using Junos telemetry interface (JTI) and remote procedure call (gRPC) services or gRPC Network Management Interface (gNMI) services. ON_CHANGE statistics are sent to an outside collector.

  The following resource paths are supported:

  - **/network-instances/network-instance/protocols/protocol/isis/interfaces/interfaces/circuit-counters/state/** (stream)
  - **/network-instances/network-instance/protocols/protocol/isis/interfaces/interface/levels/level/packet-counters/** (stream)
  - **/network-instances/network-instance/protocols/protocol/isis/levels/level/system-level-counters/state/** (stream)
  - **/network-instances/network-instance/protocols/protocol/isis/interfaces/interfaces/levels/level/adjacencies/adjacency/state/** (ON_CHANGE)
  - **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/extended-ipv4-reachability/prefixes/prefix/state/** (ON_CHANGE)
  - **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/extended-ipv4-reachability/prefixes/prefix/subtlvs/subtlv/** (ON_CHANGE)
  - **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv6-reachability/prefixes/prefix/state/** (ON_CHANGE)
  - **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv6-reachability/prefixes/prefix/subtlvs/subtlv/** (stream)

- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/extended-is-reachability/neighbors/neighbors/subTLVs/subTLVs/adjacency-sid/sid/state/** (ON-CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/extended-is-reachability/neighbors/neighbors/subTLVs/subTLVs/lan-adjacency-sid/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv4-interfaces-addresses/state/** (ON_CHANGE))
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv4-srlg/state/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv4-te-router-id/state/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv6-interfaces-addresses/state/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/router-capabilities/router-capability/subtlvs/subtlv/segment-routing-capability/state/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/state** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/area-address/state/address** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/nlpid/state/nlpid** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/lsp-buffer-size/state/size** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/hostname/state/hname** (stream)

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

- **Packet Forwarding Engine support for JTI on MX2K-MPC11E line cards (MX2010 and MX2020)**—Now supported in Junos OS Release 20.1R1, Junos telemetry interface (JTI) supports streaming of Packet Forwarding Engine statistics for MX2010 and MX2020 routers using Remote Procedure Calls (gRPC). gRPC is a protocol for configuration and retrieval of state information. This support was first introduced in Junos OS Release 19.3R2.

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

> **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

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

- **Platform, interface, and alarm sensor ON_CHANGE support on JTI (MX960, MX2020, PTX1000, PTX5000)**—Junos OS Release 20.1R1 supports platform, interface, and alarm statistics using Junos telemetry interface (JTI) and gRPC Network Management Interface (gNMI) services. You can use this feature to send ON_CHANGE statistics for a device to an outside collector.

  This feature supports the OpenConfig models:

  - **openconfig-platform.yang**: oc-ext:openconfig-version 0.12.1
  - **openconfig-interfaces.yang**: oc-ext:openconfig-version 2.4.1
  - **openconfig-alarms.yang**: oc-ext:openconfig-version 0.3.1

  Use the following resource paths in a gNMI subscription:

  - **/components/component** (for each installed FRU)
  - **/interfaces/interface/state/**
  - **/interfaces/interface/subinterfaces/subinterface/state/**
  - **/alarms/alarm/**

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

- **gRPC Dial-Out support on JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Junos OS Release 20.1R1 provides remote procedure call (gRPC) dial-out support for telemetry. In this method, the target device (server) initiates a gRPC session with the collector (client) and, when the session is established, streams the telemetry data that is specified by the sensor-group subscription to the collector. This is in contrast to the gRPC network management interface (gNMI) dial-in method, in which the collector initiates a connection to the target device.

  gRPC dial-out provides several benefits as compared to gRPC dial-in, including simplifying access to the target advice and reducing the exposure of target devices to threats outside of their topology.

  To enable export of statistics, include the **export-profile** and **sensor** statements at the [**edit services analytics**] hierarchy level. The export profile must include the reporting rate, the transport service (for example, gRPC), and the format (for example, gbp-gnmi). The sensor configuration should include the name of the collector (the server's name), the name of the export profile, and the resource path. An example of a resource path is **/interfaces/interface[name='fxp0'**.

  [See Using gRPC Dial-Out for Secure Telemetry Collection.]

- **gRPC version v1.18.0 with JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Junos OS Release 20.1R1 includes support for remote procedure call (gRPC) services version v1.18.0 with Junos telemetry interface (JTI). This version includes important enhancements for gRPC. In earlier releases, JTI is supported with gRPC version v1.3.0.

  Use gRPC in combination with JTI to stream statistics at configurable intervals from a device to an outside collector.

  [See gRPC Services for Junos Telemetry Interface.]

- **SR-TE statistics for uncolored SR-TE policies streaming on JTI (MX Series, PTX Series)**—Junos OS Release 20.1R1 provides segment routing traffic engineering (SR-TE) per label-switched Path (LSP) route statistics using Junos telemetry interface (JTI) and remote procedure call (gRPC) services. Using JTI and gRPC services, you can stream SR-TE telemetry statistics for uncolored SR-TE policies to an outside collector.

  Ingress statistics include statistics for all traffic steered by means of an SR-TE LSP. Transit statistics include statistics for traffic to the Binding-SID (BSID) of the SR-TE policy.

  To enable these statistics, include the **per-source per-segment-list** statement at the [**edit protocols source-packet-routing telemetry statistics**] hierarchy level.

  If you issue the **set protocols source-packet-routing telemetry statistics no-ingress** command, ingress sensors are not created.

  If you issue the **set protocols source-packet-routing telemetry statistics no-transit** command, transit sensors are not created. Otherwise, if BSID is configured for a tunnel, transit statistics are created.

  The following resource paths (sensors) are supported:

  - **/junos/services/segment-routing/traffic-engineering/tunnel/lsp/ingress/usage/**
  - **/junos/services/segment-routing/traffic-engineering/tunnel/lsp/transit/usage/**

  To provision the sensor to export data through gRPC services, use the **telemetrySubscribe** RPC.

  Streaming telemetry data through gRPC or gNMI also requires the OpenConfig for Junos OS module.

  [See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface, source-packet-routing, and show spring-traffic-engineering lsp detail name *name*.]

- **LLDP statistics, notifications, and configuration model for suppress-tlv-advertisement support on JTI (MX240, MX480, MX960, MX10003, PTX10008, PTX10016)**—Junos OS Release 20.1R1 provides remote procedure call (gRPC) streaming services support for attribute leaf **suppress-tlv-advertisement** under the resource path **/lldp/state/suppress-tlv-advertisement**. The following TLVs are supported, which in turn support operational state, notifications, and configuration change support:

  - port-description
  - system-name
  - system-description

- system-capabilities
- management-address
- port-id-type

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

- **CPU and NPU sensors support using JTI on MX2K-MPC11E line cards (MX2010 and MX2020)**—Junos OS Release 20.1R1 supports Junos telemetry interface (JTI) CPU and network processing unit (NPU) sensors on MX Series routers with MX2K-MPC11E line cards. JTI enables streaming statistics from these sensors to outside collectors at configurable intervals using remote procedure call (gRPC) services.

  Unlike the Junos kernel implementation in earlier Junos OS releases that support these sensors, this feature uses the OpenConfig AFT model. Because of this, there is a difference in the resource path and key-value (kv) pair output compared to the Junos kernel output.

  Use the following resource paths to export statistics:

  /junos/system/linecard/cpu/memory/

  /junos/system/linecard/npu/memory/

  /junos/system/linecard/npu/utilization/

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

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

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

- **gNMI extension compliance with JTI (MX Series)**—Starting in Junos OS Release 20.1R1, changes are qualified in the extension header for Junos telemetry interface (JTI), ensuring they are compliant with the OpenConfig gnmi.extensions.proto specification.

  See gnmi-extensions.md.]

- **gNMI-based streaming telemetry support for Packet Forwarding Engine sensors on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, gRPC Network Management Interface (gNMI) service support is available to export Packet Forwarding Engine statistics for telemetry monitoring and management using Junos telemetry interface (JTI). Using gNMI and JTI, data is exported from devices to outside collectors at configurable intervals. This feature includes support (SensorD daemon) to export telemetry data for the OpenConfig model called AFT platform.

Use the following resource paths to export sensor data for interface information and traffic, logical interface traffic, firewall filter counters, and policer counters:

- **/junos/system/linecard/interface/**
- **/junos/system/linecard/interface/traffic/**
- **/junos/system/linecard/interface/queue/**
- **/junos/system/linecard/interface/logical/usage/**
- **/junos/system/linecard/firewall/**
- **/junos/system/linecard/services/inline-jflow/**

To provision the sensor to export data through gNMI services, use the **Subscribe** RPC. The **Subscribe** RPC and subscription parameters are defined in the gnmi.proto file. Streaming telemetry data through gRPC or gNMI also requires the OpenConfig for Junos OS module.

> **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

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

Layer 2 Features

- **Supported Layer 2 features on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, the following advanced Layer 2 features are supported on MX2K-MPC11E line cards:
  - **Forwarding CoS (Q-depth monitoring)**—You can configure a Junos telemetry interface sensor that exports queue depth statistics for egress queue traffic. Telemetry data is exported directly from the line card. You can also apply one or more regular expressions to filter data. Only UDP streaming of data is supported. gRPC streaming of queue depth statistics is not currently supported. [See sensor (Junos Telemetry Interface).]
  - **Layer 2 firewall forwarding support**. [See Layer 2 Port Mirroring Firewall Filters.]
  - **Layer 2 forwarding**—IRB, VLAN handling, and Q-in-Q tunneling. [See Configuring Q-in-Q Tunneling and VLAN Q-in-Q Tunneling and VLAN Translation.] Virtual private LAN services (VPLS). [See Introduction to VPLS.] Firewall filters for Layer 2 and MAC filters. [See Layer 2 Forwarding Tables.]
  - **Multicast features**—P2MP (RSVP-TE P2MP and multipoint LDP inband) and P2MP interface support for PIM, Rosen multicast VPNs, and multicast-only fast reroute (MoFRR). [See Multicast Overview.]

> **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

- **Support for Layer 2 services with PWHT on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, some of the Layer 2 services are supported with pseudowire headend termination (PWHT) on the new MX2K-MPC11E line card.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Protocols and Applications Supported by the MX2K-MPC11E and Layer 2 VPNs and VPLS User Guide for Routing Devices.]

- **Support for basic Layer 2 features on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, MX2010 and MX2020 routers with the MX2K-MPC11E line card supports the following basic Layer 2 features:
  - Layer 2 bridging with trunk and access modes
  - MAC learning and aging
  - Handling BUM (broadcast, unknown unicast and multicast) traffic, including split horizon
  - MAC move
  - Layer 2 forwarding and flooding statics
  - Mesh groups
  - Static MAC addresses
  - MAC learning and forwarding on AE interfaces
  - Bridging on untagged interfaces
  - Basic Q-n-Q tunneling (without VLAN-translation and VLAN map operations)

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Understanding Layer 2 Bridge Domains, Understanding Layer 2 Learning and Forwarding.]

Layer 3 Features

- **Support for new MPC11E line card (MX Series)**—Starting in Junos OS Release 20.1R1, we've introduced a new MPC, MPC11E, that supports the following Layer 3 features:

  The following Layer 3 features are supported on MPC11E in 20.1R1:

  - BGP
  - IS-IS
  - Layer 3 VPN
  - OAM - LSP/VPN ping, traceroute, automatic bandwidth, and MPLS-FRR link node protection
  - OSPF
  - RIP
  - Tunnel (GRE tunnels, logical tunnels, and virtual tunnels)

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

- **Support for IPv6 Ping, IPv6 Traceroute and ECMP traceroute for Labelled-ISIS Segment Routing paths (MX Series and VMX)**— Starting in Release 20.1R1, Junos OS supports IPv6 Ping, IPv6 Traceroute, and equal-cost multipath (ECMP) traceroute for Labelled-ISIS Segment Routing paths.

Management

- **Error recovery, fault handling, and resiliency support for MX2K-MPC11E (MX2010 and MX2020)**—In Junos OS Releases 19.3R2 and 20.1R1, the MX2010 and MX2020 routers with MX2K-MPC11E line cards support error recovery, fault handling, and software resiliency. The MX2K-MPC11E line cards support detecting errors, reporting them through alarms, and triggering resultant actions. To view application level errors, use the **show trace node fpc<#> application fabspoked-pfe-redbull** command. To check the status of the card, use the **show chassis fpc pic-status** command. Use the **show chassis errors active** command to view the fault details and the **show system alarm** command to view the alarm details.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See show chassis fpc pic-status and clear chassis fpc errors.]

MPLS

- **Support for MPLS features on MX2K-MPC11E line card (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, the new MX2K-MPC11E line card supports some of the MPLS features.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Protocols and Applications Supported by the MX2K-MPC11E.]

- **Support for selective MPLS traffic mirroring (MX Series with MPC10)**—Starting in Junos OS Release 20.1R1, MX Series routers with MPC10 line cards supportelective MPLS traffic mirroring. You can apply inbound and outbound filters for the MPLS family based on MPLS-tagged IPv4 and IPv6 parameters using inner payload match conditions, and enable selective port mirroring of MPLS traffic on to a monitoring device.

  [See Understanding IP-Based Filtering and Selective Port Mirroring of MPLS Traffic]

- **Support for segment routing over RSVP forwarding adjacency (MX Series and PTX Series)**—Starting with Junos OS Release 20.1R1, we provide support for segment routing traffic to be carried over RSVP LSPs that are advertised as forwarding adjacencies in IS-IS. This feature is implemented in a network having LDP on the edge and RSVP in the core where you can easily replace LDP with IS-IS segment routing because it eliminates the need for MPLS signaling protocols such as LDP. This helps to remove a protocol from the network and results in network simplification.

  [See Understanding Segment Routing over RSVP Forwarding Adjacency in IS-IS.]

- **Support for static adjacency segment identifier for aggregated Ethernet member links on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting with Junos OS Release 20.1R1, you can configure a transit single-hop static label-switched path (LSP) for a specific member link of an aggregated Ethernet (ae) interface. The label for this route comes from the segment routing local block (SRLB) pool of the configured static label range. Configure the aggregated Ethernet member-interface name using the **member-interface** statement option at the **[edit protocols mpls static-label-switched-path *name* transit *name*]** hierarchy level. This feature is supported for aggregated Ethernet interfaces only.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See transit and Configuring Static Adjacency Segment Identifier for Aggregate Ethernet Member Links Using Single-Hop Static LSP.]

- **Support for Seamless MPLS Layer 3 features on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, MX2010 and MX2020 routers with the MX2K-MPC11E line card support the following MPLS Layer 3 features:

  - Redundant logical tunnel interfaces.
  - Pseudowire subscriber interfaces using either logical tunnel or redundant logical tunnel interfaces as anchor point.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Redundant Logical Tunnels Overview and MPLS Pseudowire Subscriber Logical Interfaces.]

- **Support for segment routing (SR) and segment routing traffic engineering (SRTE) statistics on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, MX2010 and MX2020 routers with the MX2K-MPC11E line card supports segment routing (SR) and segment routing traffic engineering (SRTE) statistics.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

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

- **CoS-based forwarding and policy-based routing to steer selective traffic over an SR-TE path (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 20.1R1, you can use CoS-based forwarding (CBF) and policy-based routing (PBR, also known as filter-based forwarding or FBF) to steer

service traffic using a particular segment routing-traffic-engineered (SR-TE) path. This feature is supported only on non-colored segment routing LSPs that have the next hop configured as a first hop label or an IP address.

With CBF and PBR, you can:

- Choose an SR-TE path on the basis of service.
- Choose the supporting services to resolve over the selected SR-TE path.

[See Example: Configuring CoS-Based Forwarding and Policy-Based Routing For SR-TE LSPs.]

- **Support for MPLS features on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, some of the MPLS features are supported on the new MX2K-MPC11E line card.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Protocols and Applications Supported by the MX2K-MPC11E.]

Multicast

- **Support for multicast forwarding on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, multicast forwarding is fully supported on MX2010 and MX2020 routers with MX2K-MPC11E line cards and Enhanced Switch Fabric Boards (SFB3).

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Multicast Overview.]

- **Next-generation multicast VPN supported on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, the MX2K-MPC11E line card supports next-generation MVPN.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Multicast Overview.]

Network Management and Monitoring

- **On-box monitoring support on the control plane (MX Series and PTX Series)**—Starting in Junos OS Release 20.1R1, you can configure on-box monitoring to monitor anomalies with respect to the memory utilization of Junos OS applications and the overall system in the control plane of MX Series and PTX Series routers.

  You can use on-box monitoring to monitor system-level memory and process-level memory to detect possible leaks. When the system is running low on memory, the process heuristic shares the prediction and you can configure the action to be taken when leaks are identified.

  See memory (system)

- **Enhanced PKI traps, log notifications, and SNMP for IPsec VPN (MX Series with USF and the SRX5000 line of devices with SPC3 card)**—Starting in Junos OS Release 20.1R1, you can enable the peer down and IPsec tunnel down traps and configure the certificate authority (CA) and local certificate traps. We've enhanced the existing IPsec VPN flow monitor MIB **jnxIpSecFlowMonMIB** to support the global data plane, active IKE SA, active IPsec SA, and active peer statistics for tunnels using IKEv2. We've also enhanced the output of the **show security ike stats** command to add additional options **(<brief> | <detail>)**. Use the **clear security ike stats** command to clear the IKEv2 statistic counters.

  [See Configure the Certificate Expiration Trap, Enterprise-Specific SNMP MIBs Supported by Junos OS, Enable Peer Down and IPsec Tunnel Down Traps, trap (Security PKI), trap (Security IKE), clear security ike stats, show security ike stats, show security ipsec statistics, show security ike security-associations, and show security ike active-peer.]

Next Gen Services

- **Support for Port Control Protocol (PCP)**—Starting in Junos OS Release 20.1R1, Next Gen Services supports the Port Control Protocol (PCP), which provides a mechanism to control how incoming packets are forwarded by upstream devices such as Network Address Translator IPv6/IPv4 (NAT64), Network Address Translator IPv4/IPv4 (NAT44), and IPv6 and IPv4 firewall devices, and mechanism to reduce application keep alive traffic.

  [See pcp-rules.]

- **Support for Traffic Load Balancer**—Starting in Junos OS Release 20.1R1, Next Gen Services support Traffic Load Balancer (TLB). TLB enables you to distribute traffic among multiple servers.

  [See Traffic Load Balancer Overview.]

- **Support for TLS transport protocol for Next Gen Services CGNAT syslog messages**—Starting in Junos OS Release 20.1R1, you can configure the transport security protocol for Next Gen Services CGNAT global syslog messages to Transport Layer Security (TLS), as well as UDP or TCP.

  TLS ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. SSL relies on certificates and private-public key exchange pairs for this level of security.

[See transport.]

- **Next Gen Services on GNFs (MX480 and MX960)**—Starting in Junos OS Release 20.1R1, guest network functions (GNFs) on MX480 and MX960 routers support Next Gen Services when the MX-SPC3 Services Processing Card is installed. You can enable Next Gen Services on a GNF by using the existing command **request system enable unified-services** at the GNF level. In a Junos node slicing setup, you can use both MX-SPC3 and MS-MPC on the same chassis but on different GNFs. However, the MX-SPC3 comes online only if you have enabled Next Gen Services on the GNF. If you have not enabled Next Gen Services, only the MS-MPC comes online.

  > **NOTE:** The MX-SPC3 does not support abstracted fabric interfaces.

  [See Enabling and Disabling Next Gen Services and request system enable unified-services.]

- **Support for URL filtering, DNS sinkhole and Juniper Sky ATP URL filtering** —Starting in Junos OS Release 20.1R1, under Next Gen Services you can configure DNS filtering to identify DNS requests for blacklisted website domains and URL filtering to determine which Web content is not accessible to users. We also support Juniper Sky ATP filtering, which is a cloud-based solution that integrates with Policy Enforcer on the Junos Space Security Director.

  [See local-category.]

OAM

- **Support for link fault management (MX2K-MPC11E)**—Starting in Junos OS Release 20.1R1, you can configure IEEE 802.3ah link fault management (LFM) for MX2K-MPC11E on MX2010 and MX2020 routers. You can also configure the following supported LFM features:
  - Discovery and link monitoring
  - Distributed LFM
  - Remote fault detection and remote loopback

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

[See Introduction to OAM Link Fault Management (LFM).]

Port Security

- **Media Access Control Security (MACsec) support on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, MACsec is supported on MX2010 and MX2020 routers with the MX2K-MPC11E line card. MACsec is an industry-standard security technology that provides secure communication for all traffic on point-to-point Ethernet links. The MPC11E supports MACsec on all 10-Gigabit Ethernet, 40-Gigabit Ethernet, and 100-Gigabit Ethernet interfaces. The supported cipher suites are GCM-AES-256 and GCM-AES-128. Only static CAK mode is supported.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

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

- **VLAN-level MACsec with unencrypted VLAN tags (MX10003 with JNP-MIC1-MACSEC)**—You can establish MACsec sessions for logical interfaces instead of physical interfaces on MX10003 routers with the JNP-MIC1-MACSEC installed. VLANs tags are now transmitted in cleartext, allowing intermediate switches that are MACsec-unaware to process VLAN tags. This feature enables MACsec encryption of point-to-multipoint VLAN connections over service provider WANs.

  [See Media Access Control Security (MACsec) over WAN.]

Routing Policy and Firewall Filters

- **Support for CCC and Layer 3 firewall forwarding on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting with Junos OS Release 20.1R1, circuit cross-connect (CCC) traffic and Layer 3 firewall forwarding features are supported on MX2K-MPC11E line cards.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See CCC Overview.]

- **Support for firewall forwarding on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, firewall forwarding is fully supported on MX2010 and MX2020 routers with MX2K-MPC11E line cards and Enhanced Switch Fabric Boards (SFB3s).

> **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

[See Filter-Based Forwarding Overview.]

- **Support for IPv6 discard interfaces (MX Series)**—Starting in Junos OS Release 20.1R1, you can configure a discard interface for IPv6 traffic. Do this at the **[edit interfaces dsc unit 0 family inet6]** hierarchy level.

  [See Configuring Discard Interfaces]

Routing Protocols

- **Support for topology-independent loop-free alternate (TI-LFA) in IS-IS for IPv6-only networks (ACX Series, MX Series, and PTX Series)**— Starting with Junos OS Release 20.1R1, you can configure TI-LFA with segment routing in an IPv6-only network for the IS-IS protocol. TI-LFA provides MPLS fast reroute (FRR) backup paths corresponding to the post-convergence path for a given failure. TI-LFA provides protection against link failure and node failure.

  You can enable TI-LFA for IS-IS by configuring the **use-post-convergence-lfa** statement at the **[edit protocols isis backup-spf-options]** hierarchy level. You can enable the creation of post-convergence backup paths for a given IPv6 interface by configuring the **post-convergence-lfa** statement at the **[edit protocols isis interface *interface-name* level *level*]** hierarchy level. The **post-convergence-lfa** statement enables link-protection mode.

  You can enable **node-protection** mode for a given interface at the **[edit protocols isis interface *interface-name* level *level* post-convergence-lfa]** hierarchy level. However, you cannot configure fate-sharing protection for IPv6-only networks.

  [See Understanding Topology-Independent Loop-Free Alternate with Segment Routing for IS-IS.]

- **Support for IP forward backup path for BGP-LS peer SIDs (MX Series)**— Starting in Junos OS Release 20.1R1, you can configure an IP forward backup path that provides protection at the local node or the point of local repair for egress peer engineering. When the primary segment goes down, the packet is forwarded to the configured IP backup path. This IP forward backup path has local node significance only. BGP does not send the IP forward backup path information to the controller in its periodic BGP LS updates. If you have configured both segment protection and IP forwarding backup path, then backup segment protection takes precedence over the IP forwarding backup path protection.

  To configure IP forward backup path for BGP LS peer segments, include the **egress-te-backup-ip-forward** option at the **[edit bgp egress-te–segment-set]**, **[edit bgp group *group-name* egress-te-node-segment]**, and **[edit bgp group *group-name* egress-te-segment adj]** hierarchy levels.

  [See egress-te-set-segment,egress-te-node-segment, and egress-te-adj-segment.]

Services Applications

- **Support for port mirroring (MX2K-MPC11E line card on MX2010 and MX2020 routers)**—In Junos OS Releases 19.3R2 and 20.1R1, you can configure port mirroring on the MX2K-MPC11E line card to mirror a copy of a packet to a configured destination, in addition to the normal processing and forwarding of the packet. The MX2K-MPC11E supports IPv4 (inet) and IPv6 (inet6) address families only.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Configuring Port Mirroring.]

- **Support for tunnel interfaces (MX2K-MPC11E line card on MX2010 and MX2020 routers)**—In Junos OS Releases 19.3R2 and 20.1R1, Junos OS supports three tunnel interfaces: generic routing encapsulation (GRE) tunnel, logical tunnel (LT), and virtual tunnel (VT) on the MX2K-MPC11E line card.

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

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Tunnel Services Overview.]

- **Fabric support on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, the MX2K-MPC11E line card is introduced. It is composed of 8 Packet Forwarding Engines per FPC. Each Packet Forwarding Engine on the MX2K-MPC11E line card has 3 fabric planes per SFB, which is a total of 24 fabric planes. All Packet Forwarding Engines have fabric connectivity with the SFB3. The fabric links are monitored for cyclic redundancy check (CRC) errors. Each Packet Forwarding Engine supports 500G fabric throughput when all 24 fabric planes are operational.

  > **NOTE:**
  > - Fabric redundancy is not supported on MX2K-MPC11E line card. The MX2K-MPC11E line card interoperates only with SFB3.
  > - The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

[See Protocols and Applications Supported by the MX2K-MPC11E.]

- **Support for local preference when selecting forwarding next hops for load balancing on MPC11E (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, you can have traffic flows across aggregated Ethernet or redundant logical-tunnel interfaces prefer local forwarding next hops over remote ones, for example to ensure that the overall load on the fabric is reduced.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See local-bias.]

- **Inline J-Flow support for EVPN traffic (MX Series with MPC10 and MPC11)**—Starting with Junos OS Release 20.1R1, you can use inline J-Flow sampling for the bridge family. You can monitor Inline J-Flow traffic hitting the bridge family and report the necessary fields in either Version 9 or IPFIX format. The new bridge family under the **forwarding-options sampling instance** hierarchy monitors all traffic hitting the VPLS or bridge family.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Understanding Inline Active Flow Monitoring.]

- **Configure next-hop-based dynamic tunnels on MX2K-MPC11E line card (MX2010 and MX2020 routers)**—In Junos OS Releases 19.3R2 and 20.1R1, on MX2010 and MX2020 routers with an MX2K-MPC11E line card, you can configure next-hop-based dynamic tunnels for the following configurations:

  - MPLS-over-UDP—You can configure a dynamic MPLS-over-UDP tunnel that includes a tunnel composite next hop.

    In a dynamic tunnel configuration, where the Routing Engine forwards a lot of routes to the Packet Forwarding Engine, the FIB convergence may take more time resulting in traffic loss. Also, when you restart an FPC restart in a dynamic tunnel configuration, traffic flow may not resume.

  - MPLS-over-GRE—You can configure MPLS LSPs to use generic routing encapsulation (GRE) tunnels to cross routing areas, autonomous systems, and ISPs.

    > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See dynamic-tunnels.]

- **Support for inline active flow monitoring on (MPC11E line cards on MX240, MX480, and MX960)**—Starting in Junos OS Release 20.1R1, you can perform inline flow monitoring to support:
  - MPLS, MPLS-IPv4, and MPLS-IPv6
  - IPv4 or IPv6 traffic on next-hop based GRE tunnels and ps interfaces

  Both IPFIX and V9 formats are supported.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Understanding Inline Active Flow Monitoring.]

- **Support for Two-Way Active Measurement Protocol (TWAMP) on MX2K-MPC11E line card (MX240, MX480, and MX960)**—Starting in Junos OS Release 20.1R1, the MX2K-MPC11E line card supports TWAMP. You can use the TWAMP-Control protocol to set up performance measurement sessions between a TWAMP client and a TWAMP server, and use the TWAMP-Test protocol to send and receive performance measurement probes. Configuring the TWAMP client instance to use si-x/y/z as the destination interface (which enables inline services) is not supported if the router has an MX2K-MPC11E installed in the chassis. You can configure only the none authentication mode on the line card.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Understanding Two-Way Active Measurement Protocol on Routers.]

- **L2TPv2 silent failover on peer interface for L2TPv2 subscriber services on MX2K-MPC11E line card (MX2010 and MX2020 routers)**—In Junos OS Releases 19.3R2 and 20.1R1, you can configure L2TPv2 silent failover and peer interface support for L2TPv2 subscriber services on MX2K-MPC11E line card.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Peer Resynchronization After an L2TP Failover.]

- **Port mirroring support on MX2K-MPC11E (MX2010 and MX2020 routers)**—In Junos OS Releases 19.3R2 and 20.1R1, you can configure port mirroring on the MX2K-MPC11E line card. You can configure port mirroring for the CCC, bridge, and family any only.

> **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

[See Understanding Port Mirroring.]

- **FlowTapLite support on MPC10E (MX240, MX480, and MX960 routers)**—Starting in Junos OS Release 20.1R1, you can configure FlowTapLite on the MPC10E line card.

  [See Configuring FlowTapLite on MX Series Routers and M320 Routers with FPCs.]

- **Support adaptive load balancing (ALB) for ECMP next hops (MX Series)**—Currently, adaptive load balancing for ECMP next hops is limited to a single Packet Forwarding Engine. Hence, traffic is restricted to a single Packet Forwarding Engine and impacts the flexibility and redundancy. Starting in Junos OS Release 20.1R1, you can configure adaptive load balancing for ECMP next hops across multiple ingress Packet Forwarding Engines on the same line card for even distribution of the traffic and redundancy. The behavior is default starting with Junos OS Release 20.1R1 and you cannot choose to configure back to the behavior prior to Junos OS Release 20.1R1. Also, the behavior is not applicable when you configure adaptive load-balancing and locality-bias together.

  To configure adaptive load balancing for ECMP next hops, configure the **ecmp-alb** command under the **[edit chassis]** hierarchy level.

  [See ecmp-alb].

Software Defined Networking

- **Delegate segment routing LSPs to a PCE (MX Series)**—Starting in Junos OS Release 20.1R1, you can enable a Path Computation Client (PCC) to delegate locally configured IPv4 non-colored segment routing LSPs to a Path Computation Element (PCE) controller. The PCE controls the delegated LSPs and can modify LSP attributes for traffic steering.

  A PCC with delegation capability can take back control of the delegated segment routing LSPs from the PCE when the PCEP session goes down; the LSPs would otherwise be deleted from the PCC. You can thus ensure LSP data protection by averting a situation where packets are silently discarded or dropped (also known as a traffic black-hole condition).

  [See Segment Routing for the Path Computation Element Protocol Overview and Example: Configuring Path Computation Element Protocol for SPRING-TE LSPs.]

Subscriber Management and Services

- **Support for BNG M:N subscriber redundancy over pseudowire interfaces (MX Series)**—Starting in Junos OS Release 20.1R1, you can configure BNG M:N redundancy using pseudowire redundancy in addition to using VRRP redundancy. The pseudowire redundancy method is supported for IP/MPLS network and Layer 2 VPN scenarios using pseudowire tunnels. These scenarios support dynamic N:1 VLANs.

  [See M:N Subscriber Redundancy Overview.]

- **Distributed denial of service protection on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, the MX2K-MPC11E line cards support DDoS protection.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

  [See Protocols and Applications Supported by the MX2K-MPC11E.]

- **Subscriber services uplink support on MX2K-MPC11E line cards (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, you can use the MX2K-MPC11E line cards for uplink connections to the core network. This support requires you to enable enhanced subscriber management.

  > **NOTE:** The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

[See Protocols and Applications Supported by the MX2K-MPC11E.]

- **Support for managing policy and charging rules function (PCRF) server errors (MX Series)**—Starting in Junos OS Release 20.1R1, you can configure the router to reinitialize the PCRF session when triggered by certain PCRF server errors that result in a state mismatch between the server and the router. You can also configure the router to generate an extended session ID that is universally unique by appending a 32-bit session stamp based on the current UTC time when the router creates the CCR-GX-I.

  [See Understanding Gx Interactions Between the Router and the PCRF.]

System Management

- **Precision Time Protocol (PTP) and IRB support on MPC7E line cards (MX240, MX480, and MX960)**—Starting in Junos OS Release 20.1R1, we support PTP over IRB on master interface configurations for MPC7E line cards. This release also supports the configuration of aggregated Ethernet over IRB. We've also added **disable-lag-revertive-switchover** statement at a global level. This configuration enables nonrevertive switchover for a LAG.

  NOTE:
  - Two-step clock mode is not supported.
  - PTP aggregated Ethernet child link switchover is not hitless, in both negotiated and nonnegotiated cases, in scenarios with aggregated Ethernet, because the client goes through a resynchronization phase. When unicast negotiation is enabled, the PTP backup clock starts fresh with new negotiation messages using the secondary link whenever the current active link goes down.
  - Aggregated Ethernet with mixed-speed child links is not supported over IRB.

  [See Configuring Precision Time Protocol Over Integrated Routing and Bridging.]

- **Restrict option under NTP configuration is now visible (ACX Series, QFX Series, MX Series, PTX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the **noquery** command under the **restrict** hierarchy is now available and can be configured with a mask address. The **noquery** command is used to restrict ntpq and ntpdc queries coming from hosts and subnets.

  [See Configuring NTP Access Restrictions for a Specific Address.]

User Interface and Configuration

- **Synchronous Ethernet support for MPC11E (MX2010 and MX2020)**—Starting in Junos OS Release 20.1R1, Synchronous Ethernet is supported on the MPC11E.

  NOTE: Junos OS dose not support synchronous Ethernet clock recovery from MIC and Precision Time Protocol (PTP).

  NOTE: The MX2K-MPC11E line card is also supported in Junos OS 19.3R2 and later 19.3 releases. It is not supported in any Junos OS 19.4 releases.

[See Synchronous Ethernet Overview.]

SEE ALSO

What's Changed

IN THIS SECTION

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

Interfaces and Chassis

- **Displaying accurate aggregate drop statistics (MX Series)**—Starting in Junos OS Release 20.1R1, you can view the accurate aggregate drop statistics when a packet drop is seen on an aggregated Ethernet Interface by using the **show interfaces extensive** command. In earlier releases, the **show interfaces extensive** command did not display accurate aggregate drop statistics. Only the individual aggregate child interface displayed accurate drop statistics.

Network Management and Monitoring

- **Change in startup notification after GRES (MX Series routers)**– Starting in Junos OS Release 20.1R1, the master Routing Engine sends a **coldStart** notification when a device comes up. The master Routing Engine also sends **warmStart** notifications for subsequent restarts of the SNMP daemon. After graceful routing engine switchover (GRES) the new master Routing Engine sends a single **warmStart** notification and the backup Routing Engine does not send any notification. In earlier releases, after GRES, the new master RE would sometimes send two notifications or a single notification. Of these, the first notification was always a **coldStart** notification and the second was either a **coldStart** notification or a **warmStart** notification.
- **Enhancement to the show SNMP mib command**– In Junos OS Release 20.1R1, and later, a new option, **hex**, is supported to display the SNMP object values in the hexadecimal format. In earlier releases, the **show snmp mib** command displays the snmp object values in ASCII and decimal format only.

  See show snmp mib

Services Applications

- **Update to CLI option for configuring the version number to distinguish between currently supported version of the Internet draft draft-ietf-softwire-map-03**—In Junos OS Release 20.1R1, the **version-3** option under the **[edit services softwire softwire-concentrator map-e]** hierarchy for configuring the version number to distinguish between currently supported version of the Internet draft draft-ietf-softwire-map-03 is optional. In the earlier Junos OS releases, if you did not configure the **version-3** option, the configuration resulted in an error.

  [See map-e.]

Subscriber Management and Services

- **Single memory map applies to configuration and schema databases (MX Series)**—Starting in Junos OS Release 20.1R1, the Junos OS configuration database and the schema database share the same memory space. This means that when you set the maximum database size, the result is the total memory available to both of these databases. In earlier releases, the schema database is separate and fixed in size.

  [See Configuring Junos OS Enhanced Subscriber Management.]

SEE ALSO

What's New | 71

Known Limitations | 105

Open Issues | 108

Resolved Issues | 115

Documentation Updates | 133

Migration, Upgrade, and Downgrade Instructions | 134

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

- In some scenarios with MPC, the following major alarm and following messages are generated: **messages log: fpcx XQCHIP(46):XQ-chip[0]: DROP protect_regs error (status=0x8) alarmd[3158]: Alarm set: FPC color=RED, class=CHASSIS, reason=FPC x Major Errors Major alarm set, FPC x Major Errors fpcx XQCHIP(46):XQ-chip[0]: DROP protect_regs error (status=0x8) cli> show chassis alarms 1 alarms currently active Alarm time Class Description 2019-01-25 15:18:03 UTC Major FPC x Major.**

  Despite the major alarm set, this error is due to the Unknown Error Address logged in hardware to the DQ underrun. This message is harmless and has no service impact. PR1303489

- The MX104 router has the following limitations in error management:
  - The **show chassis fpc error** command is not available for MX104 in Junos OS Releases 13.3R7, 15.1R2,14.1R5,14.2R4, 13.3R8, and later.
  - Junos OS does not initiate restart of the system on encountering a fatal error.
  - Although you can configure **disable-PFE** for major errors action, Junos OS does not disable its only Packet Forwarding Engine on encountering a major error. PR1413314
- The Routing Engine interprets any input from the console port as interrupts. Depending on the frequency, console noise impacts the Routing Engine interruption handling to different extents, even with the current mechanism. When the interrupt frequency is too high for the Routing Engine to handle, the impact might vary from the line card reboot (partial impact) to the Routing Engine reboot (chassis-wide impact). PR1436386
- In a scaled scenario where the Routing Engine pushes a lot of routes to the Packet Forwarding Engine in the presence of the dynamic tunnel configuration, FIB convergence might take more time, leading to traffic drops. PR1454817
- Dynamic SR-TE tunnels does not get automatically re-created at the new master Routing Engine after the Routing Engine switchover. PR1474397
- The control peer PFCP heartbeat request timeout window must be greater than 90 seconds. PR1459135
- The traffic on GRE interface on both ingress and egress cannot be Layer 2 mirrored. PR1462375

- The following error message is issued when the connection between aftman and aft-ulcd is dropped: **[Error] aft-ipc: AFT-ULCD IPC: Program will exit - ERROR MESSAGE.** PR1467246
- The aftd hogs on executing the clear VPLS table and MACs are not learned for less than 5 minutes. PR1473334

Infrastructure

- The Juniper Routing Engine with HAGIWARA CF card installed, after upgrading to Junos OS Release 15.1 and later, the following error message might appear on the log: **smartd[xxxx]: Device: /dev/ada1, failed to read SMART Attribute Data** PR1333855

Platform and Infrastructure

- Traffic might drop due to the memory error of QX-chipset MPC. PR1197475
- Interface-group based firewall filters used at MX Series router with the VPLS and BRIDGE logical interfaces hosted by an MPC might work unpredictably. PR1216201

Services Applications

- Currently, while configuring a DNS filter profile at the **[edit services web-filter profile *profile-name* dns-filter-template]** hierarchy level, you can configure a maximum of number of 32 DNS filter templates. However, for a profile configured under **[edit services web-filter profile *profile-name* security-intelligence-policy]** hierarchy level, you can configure more than 32 templates.

  [See dns-filter-template and security-intelligence-policy].

Subscriber Management and Services

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

As a workaround, you must configure the CPE to send a single solicit message for both IA_NA and IA_PD when the other configuration elements are present. PR1441801

VPNs

- In an MVPN scenario with static lsp mapping type 3, the route withdraw behavior might differ. PR1466122

SEE ALSO

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.

EVPN

- Duplicate packets in EVPN scenario are seen because a nondesignated forwarder is sending an inclusive multicast packet to the PE-CE interface after MAC lookup. PR1245316
- In an EVPN scenario with nonstop active routing (NSR) enabled, the rpd crashes and generates core files on the backup Routing Engine when any configuration changes on the master Routing Engine. PR1336881
- With Junos OS Release 19.3R1, the VXLAN OAM host-bound packets are not throttled with DDoS policers. PR1435228
- EVPN-VXLAN core isolation does not work when the system reboots or the routing restarts. PR1461795
- The ARP entry gets deleted from the kernel after adding and deleting the virtual-gateway-address. PR1485377

Forwarding and Sampling

- For Junos OS Releases 18.4R1 and 18.3R2, if an IPv4 prefix is added on a prefix-list referred by an IPv6 firewall filter, the following log message is not seen: **Prefix-List [Block-Host] in Filter [Protect_V6] not having any relevant prefixes , Match [from prefix-list Block-Host] might be optimized.** PR1395923

General Routing

- The fxp0 is marked as **Dest-route-down** because of specific operations such as disabling and enabling operations. PR1052725
- The input errors on MX150 might be zero under the **show interfaces extensive** output when there are CRC or Align errors on the interface. PR1485706
- The **show ptp statistics detail** command shows incorrect values for the delay request and response packets. PR1489711
- Loss in subscriber might be seen post ISSU for DHCPv6 server subscribers over PPPoE. PR1489954
- In the MX-VC platforms, setting or deleting a VC port causes other VC ports on the same FPC or MIC slot to bring the link in the **Down** state for a few seconds, possibly interrupting communication with the other member chassis. PR1493699
- Incase of G.8273.2 measurement of asymmetric combination of port speeds involving 40-Gigabits Ethernet, cTE metrics of 60-120ns in certain trials are observed. PR1488549
- On a vMX platform, the performance of the Intel X710 NIC is lower compared to the performance of the Intel 82599 NIC. PR1281366

- Because a vendor does not use chained CNH, using the feature does not bring in a lot of gain, because TCNH is based on an ingress rewrite premise. Without this feature, things work just fine. PR1318984
- Changing framing modes on a CHE1T1 MIC between E1 and T1 on a MPC3E NG HQoS line card causes the PIC to go offline. PR1474449
- In a Message Queuing Telemetry Transport (MQTT) scenario, about 4000 KB of memory leakage might be seen every 30 seconds. However, on very long runs, this leakage uses up high memory, which can indirectly impact other running daemons. PR1324531
- When the FPC boots (either during unified ISSU, router reboot, or FPC restart), I2C timeout errors for SFP are onserbed. These errors are seen because of the incomplete I2C action as the device was busy. After the FPC is up, all the I2C transactions to the device were normal and there were no periodic failure. There is no functional impact and these errors can be ignored. PR1369382
- On the MPC10E and MPC11E line cards, the IPv6 local statistics are counted against the IPv6 transit traffic statistics as well. PR1467236
- Invalid packets are dropped by dut with tcc encapsulation configuration as intended but the statistics counters get incremental. PR1481698
- With regard to FPC restarts or Virtual Chassis splits, the design of MX Series Virtual Chassis infrastructure relies on the integrity of the TCP connections. The reactions to failure situations might not be handled gracefully. This results in TCP connection timeouts because of jlock hog crossing the boundary value (5 seconds), which causes bad consequences in MX Series Virtual Chassis. Currently, there is no other easy solution to reduce this jlock hog besides enabling marker infrastructure in the MX Series Virtual Chassis setup. PR1332765
- On the MX2010 and MX2020 routers equipped with SFB2, some error logs might be seen. PR1363587
- On the MX480 and EX9208 devices, a few XE interfaces go down with the following error message: **if_msg_ifd_cmd_tlv_decode ifd xe-0/0/0 #190 down with ASIC Error.** PR1377840
- The traffic destined to the VRRP VIP drops because the filter is not updated to the related logical interface. PR1390367
- Traffic statistics are not displayed for the hybrid access gateway session and tunnel traffic. PR1419529
- Traffic drops after the FPC reboots with the aggregated Ethernet member links deactivated by the remote device. PR1423707
- When you run the **show route label X | display json** command, two **nh** keys are present in the output. PR1424930
- On the dual Routing Engines of the MX Series platforms with subscriber management, the replication daemon (repd process) might crash after booting for the first time with a newly installed Junos OS release. The repd process synchronizes subscriber information across Routing Engines, so normally the repd crash has no impact on the live service. PR1434363
- MPC10E 3D MRATE-15xQSFPP : Layer 2 over GRE is not supported in Junos OS Release 19.3R1. Even though the configuration gets committed, the feature will not work. PR1435855

- Interface hold-down timers cannot be achieved for less than 15 seconds on MPC11E at FRS. PR1444516
- The **Mixed Master and Backup RE types** alarm is observed when MX2008 with RE-MX2008-X8-128G detects backup Routing Engine as RE-MX2008-X8-64G. PR1450424
- Physical interface policers are not supported in Junos OS Release 19.3 for MPC11. PR1452963
- Issues with CLI command are observed after ANCP restarts, before ANCP neighbor reestablishes, and before receiving the port-ups. PR1453837
- With logical system configuration, filter-based GRE encapsulation does not work. PR1456762
- On the MPC11E line card, the FIB download rates are lower than MPC10E by 30 percent. PR1456816
- On the MPC11E line card, the following error messages are seen when the line card is online: **i2c transaction error (0x00000002).** PR1457655
- With the scale filter-based forwarding (FBF) configuration, two instances seem unable to forward the traffic to the respective routing instances. It appears that the FBF programming is incorrect for these two FBF instances. PR1459340
- Some threads of the CPU information might not get exported for the CPU memory sensor. PR1461155
- Backport jemalloc profiling CLI to support all Junos OS Releases where jemalloc is present. PR1463368
- The MPC2E-NG or MPC3E-NG card with specific MIC might crash after a high rate of interface flaps. PR1463859
- The following syslog error messages are harmless and expected during ISSU or GRES or FPC offline/online scenarios: **[Oct 3 08:48:35.836 LOG: Err] ifl ps240.1 (1712): child ifl lt-1/0/0.32767 (7709) already there [Oct 3 08:48:35.836 LOG: Err] IFRT: 'Aggregate interface ifl add req' (opcode 87) failed [Oct 3 08:48:35.836 LOG: Err] ifl 1712, child ifl 7709; agg add failed.** PR1464524
- BFD session might flap when the session moves into an aggressive interval after coming up from a slow or non aggressive interval. PR1465285
- On the MPC11E line card, the **DOM MIB** alarm for the channelized 10-Gigabit Ethernet interface does not show any alarm for LF/RF. PR1467446
- Not able to get the service sessions when NAT64 is configured with destination-prefix length of 32. PR1468058
- In Junos OS Release 16.2R1 and later, if commit is executed after commit check, the daemon (for example, dhcpd and sampled) might not get started even after the related configuration is successfully committed. PR1468119
- FPC online might take additional time during movement of MPC11 FPC from one GNF to another GNF. PR1469729
- With BGP rib-sharding and update-threading, traffic drops 100 percent in the BGP Layer 3 VPN streams, after the removal or restoration configuration. PR1469873

- When Layer 2 bridge domain is configured and traffic is flowing only on one particular interface, the MACsec statistics might be updated incorrectly on other channelized MACsec interfaces on the same port group. PR1472464
- For the MPC10E card line, the IS-IS and micro BFD sessions do not come up during baseline. PR1474146
- Upon external X86 node slicing server reboot, the host SNMP configuration gets overwritten by the JDM SNMP configuration settings. PR1474349
- In some scenarios with the PTP hybrid mode and MPC5E line card, continuos resetting of the Playback Engine log message occurs. The Playback Engine resides inside MPC5E FPGA and it is responsible for maintaining the PTP states. PR1420335
- On the MX Series platforms, if the clock frequency slowly change on CB0 (slow drift), the clock source for MPC-3D-16XGE-SFPP might not be changed to CB1, which cause interfaces on it to go down and remain in the **Down** state. PR1433948
- With multiple different fixed-sized traffic streams configured at 1000000 fps (40 gbps combined rate) on an aggregated Ethernet0 along with another independent aggregated Ethernet (aggregated Ethernet1, 50 percent line rate 4 streams bi-directional => 118 gbps combined traffic rate) both hosted on a single Packet Forwarding Engine instruction of MPC11E line card, causes small varying packet drops every iteration on the aggregated Ethernet1 on disabling the aggregated Ethernet0. The drops might vary from 200 to certain 1000 frames. PR1464549
- The BGP sessions over the ps interfaces anchored over rlt might flap during ISSU. PR1478693
- The Next-Gen Services MX-SPC3 service card does not come online automatically when the junos-vmhost image is installed on the Next-Generation Routing Engine (NG-RE): RE-S-X6-64G-UB. PR1482334
- BFD over Layer 2 VPN or Layer 2 circuit does not work because of the SDK upgrade to version 6.5.16. PR1483014

Infrastructure

- The following error message might be seen after an upgrade: **invalid SMART checksum.** PR1222105

Interfaces and Chassis

- Spontaneous jpppd generates core files on the backup Routing Engine in a longevity test at **../../../../../../src/junos/usr.sbin/jpppd/pppMain.cc:400**. PR1350563
- The SFP index in Packet Forwarding Engine starts at 1, while the port numbering starts at 0. This causes confusion in the log analysis. PR1412040

Junos Fusion Provider Edge

- On a Junos fusion system, intermediate traffic drop is sometimes seen between AD and SD when sFlow is enabled on the ingress interface. When sFlow technology is enabled, the original packet gets corrupted for those packets that hit the sFlow filter. Because of few packets transmitted from the egress of AD1 are short of FCS (4 bytes) + 2 bytes of data drops occur. The normal data packets are of size 128 bytes while the corrupted packet is 122 bytes. PR1450373

Layer 2 Ethernet Services

- When you revert from an Enhanced Switch Control Board (SCBE) upgrade, the SCB fails with the following error message: **CHASSISD_FASIC_PIO_READ_ERROR.** PR980340
- The DHCP DECLINE packets are not forwarded to the DHCP server when **forward-only** is set within **dhcp-reply**. PR1429456
- DHCPv6 renew do not occur as expected at the ALQ backup relay. PR1489219

MPLS

- The rpd generates core files at **hbt_iterate_next, ldp_purge_unknown_tlv_temp_tree**. PR1210526
- If the two directly connected BGP peers runs on top of a LSP and the MTU of the IP layer is smaller than the MTU of the MPLS layer; plus the BGP packets from the host have the DF bit set, the BGP session may ight keep flapping because of wrong usage of the TCP-MSS. PR1493431
- The RSVP interface bandwidth calculation rounds up. PR1458527

Platform and Infrastructure

- In an EVPN and VPLS scenario, the packet gets corrupted at an ingress Packet Forwarding Engine. PR1300211
- When the REST service configuration is modified, for example, the REST service is configured and then deleted for multiple times, the system might become unresponsive, even to SSH and console. This issue has service impact. PR1461021
- If the interface is newly added as CE interface, the existing bum traffic can be looped. Loop prevention features is designed to start working whenever a new CE interface is added by configuration. But the existing bum traffic can be distributed to a new CE interface earlier before enabling the loop prevention feature. PR1493650
- Due to timing condition, the dead next-hops in the flood group of EVPN-MPLS are seen after remote PEs bounce. This affects the raffic flooding to remote EVPN PEs. PR1484296

On the MX150 and vMX platform, the VXLAN packet might get discarde because the flow caching does not support VXLAN when the flow caching enabled. PR1466470

- On MX Series routers with MPCs, the unicast traffic might drop when the destination is reachable over an integrated routing and bridging (IRB) interface and a label-switched interface (LSI) with two next hops. PR1420626
- On the MX-VC setup, if traffic goes through a VCP (virtual chassis port) port and forwards to an egress port to the destination, while the traffic is handled entirely by the same PFE, MAC malformation might occur. PR1491091
- On the EX9208 and MX480 devices, traffic loss is observed if the ingress and egress ports are in different FPCs. PR1429714
- For the bridge domains configured under an EVPN instance, the ARP suppression is enabled by default. This enables the EVPN to proxy the ARP and reduces the flooding of ARP in the EVPN networks. As a result, the **storm-control** does not affect the ARP packets on the ports under such bridge domain. PR1438326
- On the MX Series router with SP-style, traffic gets looped with the logical interface flapping. PR1485100
- A dual Routing Engine Junos node slicing GNF with no GRES configured and with a **system internet-options no-tcp-reset drop-all-tcp** configuration might enter the dual backup Routing Engine state upon manual GNF Routing Engine mastership switchover attempt with the **request chassis routing-engine master [acquire|release|switch]** command from either GNF Routing Engine CLI. PR1456565
- While the SNMP-Agent polls round-trip time (RTT) related to OIDs from a router running Junos OS, such as **pingResultsAverageRtt**, the router might respond with zero (0) value even though there is no RPM ping failure. The following objects might be impacted: **iso.3.6.1.2.1.80.1.3.1.4 -> pingResultsMinRtt iso.3.6.1.2.1.80.1.3.1.5 -> pingResultsMaxRtt iso.3.6.1.2.1.80.1.3.1.6 -> pingResultsAverageRtt iso.3.6.1.2.1.80.1.3.1.7 -> pingResultsProbeResponses iso.3.6.1.2.1.80.1.3.1.9 -> pingResultsRttSumOfSquares.** PR1458983
- When traffic is received from 1000 different VRF instances on PE from CE devices, a , few flows are dropped at the PE device. PR1460471
- Sometime high CPU utilization is observed in MPC 3D 16x 10GE after ISSU. PR1461715
- A few OAM sessions are not established with the scale EVPN ETREE and CFM configurations. PR1478875

Routing Protocols

- In the BGP environment, the Ukern memory leaks and the core crashes. PR1366823
- Even when the **protocols mpls traffic-engineering bgp-igp** command is configured, the UDP tunnel routes are not added to inet.0. The UDP tunnel routes are added only to inet.3 table whether the command is configured or not. PR1457426

- In a next-generation MVPN setup, when using MPC10 on egress an PE device with load-balancing join of multiple groups in C_VPN, the egress PE device might not receive multicast traffic. PR1476969
- If a manually configured rib-group or automatically generated rib-group (through **family inet labeled-unicast resolve-vpn**) is used to copy inet.0 (IP routing table) routes to inet.3 (MPLS routing table), the process rpd might continuously generate soft core files after **protocols bgp path-selection always-compare-med** is configured. PR1487893

Subscriber Access Management

- Verifying deleted services through CoA when the specified family-type has been deactivated fails because of the incorrect numbers of the active service sessions. PR1479486

VPNs

- Traffic loss is observed while verifying multicast route with VT for VPNA. PR1460480
- In the MVPN environment with SPT-only option, if the source or receiver is connected directly to the c-rp PE device and the MVPN data packets arrive at the c-rpce PE device before its transition to SPT, the MVPN data packets might be dropped. PR1223434

SEE ALSO

What's New | **71**

What's Changed | **103**

Known Limitations | **105**

Resolved Issues | **115**

Documentation Updates | **133**

Migration, Upgrade, and Downgrade Instructions | **134**

Resolved Issues

IN THIS SECTION

This section lists the issues fixed in Junos OS Release 20.1R1 for MX Series routers.

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

Application Layer Gateways

- SIP messages that needs to be fragmented might get dropped by the SIP ALG. PR1475031

Authentication and Access Control

- The LLDP packets might get discarded on all Junos OS platforms. PR1464553

Class of Service (CoS)

- The MX Series generated OAM/CFM LTR messages are sent with a different priority than the incoming OAM/CFM LTM messages. PR1466473

- Unexpected traffic loss might be discovered in certain conditions under in a Junos fusion scenario. PR1472083
- The MX10008 and MX100016 routers might generate cosd core files after executing the **commit/commit check** command if the **policy-map** configuration is set. PR1475508

EVPN

- Traffic received from VTEP is dropped if the VNI value used for type-5 routes is greater than 65,535. PR1461860
- Rpd might crash with the EVPN-related configuration changes in a static VXLAN to MPLS stitching scenario. PR1467309

Forwarding and Sampling

- Traffic errors do not get policed as expected after being locally switched for VLAN 100 and 101, while verifying the selective local-switching functionality with 4000 VLANs. PR1436343
- The pfed might crash and not be able to come up on the PTX Series or TVP based platforms. PR1452363
- The following syslog error messages are seen: **pfed: rtslib: ERROR received async message with no handler: 28.** PR1458008
- The following false warning message is seen on commit (commit check) after upgrading to Junos OS Release 19.2R2-S1.4: **warning: vxlan-overlay-load-balance configuration for forwarding options has been changed.** PR1459833
- On an MX Series router, the following logs are seen: **L2ALD_MAC_IP_LIMIT_REACHED_IF: Limit on learned MAC+IP bindings reached for .local.1048605; current count is 1024**. PR1462642
- Type 1 ESI/ or AD routes are not generated locally on EVPN PE devices in all-active mode. PR1464778
- On the MX10008 and MX10016 routers, policer bandwidth-limit cannot be set higher than 100-Gigabit Ethernet. PR1465093
- An output bandwidth-percent policer with logical-bandwidth-policer applied to an aggregated Ethernet bundle along with an output-traffic-control-profile has incorrect effective policing rate. PR1466698
- Traffic might be forwarded into the default queue instead of the right queue when the VPLS traffic has three or more VLAN tags with VLAN priority 5. PR1473093
- The filter might not be installed if the **policy-map xx** is present under the filter. PR1478964

General Routing

- The severity of the following error is reduced from fatal to major: **XR2CHIP_ASIC_JGCI_FATAL_CRC_ERROR.** PR1390333
- On the MX240, MX480, or MX960 router with SCB3E, swapping MPC10E line card with MPC7E line card in the same FPC slot results in fabric errors, which causes system-wide traffic impact. PR1491968
- After restarting the routing or rpd process, sometimes the sensor statistics is not reset. After the rpd process restarts, the sensor do not reset and traffic statistics increases on the existing value. PR1458107
- A newly added LAG member interface might forward traffic even though its micro BFD session is down. PR1474300
- In a configuration mode, when you ask for command completion help for the **co-ordinate configuration** statement at the **[edit protocols lldp-med interface location]** hierarchy level, you see that the word value is misspelled in the help text. PR1486327
- On the MX104 platform with any 2-port license installed on the 10-Gigabits Ethernet interfaces and phy-timestamping enabled in PTP, PTP might not work. PR1421811
- Default configuration does not create any logical interfaces and LLDP cannot discover neighbor for those interfaces which logical interface is not configured explicitly in the Junos OS configuration. PR1436327
- The failover time for the LACP link protection might be more than 2 seconds on the MPC11E line card. PR1464652
- The following constant messages flooding in log is observed: **summit_pic_port_profile_isvalid: VALID Port profile.** PR1464879
- The **high-cos-queue-threshold** range is changed to [uint 0 .. 90;]. PR1390424
- NAPT66 pool split is not supported with AMS; thus commit must fail with IPv6 pool in AMS. PR1396634
- The non existent subscribers might appear in the **show system resource-monitor subscribers-limit chassis extensive** output. PR1409767
- Changing CAK and CKN multiple times within a short interval (around 5 minutes) sometimes show the security MACsec connection's inbound and outbound channel display with more than one active AN. But on the Packet Forwarding Engine hardware side, the correct AN and SAK is programmed and MKA protocol from both ends transmits the correct and latest AN on each hello packet. You should not see any traffic drop due to this display issue. PR1418448
- Certain JNP10008-SF and JNP10016-SF Switch Interface Boards (SIBs) manufactured between July 2018 and March 2019 might have incorrect core voltage setting. PR1420864
- The jnxFruState shows value as 10 for Routing Engine instead of 6 in response to .1.3.6.1.4.1.2636.3.1.15.1.8.9.1.0.0. PR1420906
- Ports might get incorrectly channelized if they are already of 10-Gigabit Ethernet and they are channelized to 10-Gigabit Ethernet again. PR1423496

- Observing NPC core files at **trinity_rtt_hw_bulk_helper**, **trinity_rt_delete**, rt_entry_delete_msg_proc (rt_params=0x48803bd8) at **../../../../../../../../src/pfe/common/applications/route/hal/rt_entry.c:5210**. PR1427825
- The following syslog error message is observed: **Err] dfw_abstract_issu_stats_counters_restore:2222 Failed to find Index = 4613734? during ISSU with 19.3I-20190409_dev_common.0.2212.** PR1429879
- The routers that are configured with the protect core file might send IPfix sampling packets with the incorrect next-hop information. PR1430244
- The l2cpd process might crash and generate a core file when the interfaces flap. PR1431355
- MicroBFD 3x100ms flap is observed upon inserting a QSFP in another port. PR1435221
- ZF interrupts for out-of-range destination Packet Forwarding Engine INTR for Gnt is observed when the MPC6 or MPC9 line card is brought up. PR1436148
- ISSU fails from the legacy Junos OS Release 19.1R1 images. PR1438144
- Incorrect values are observed in the **JUNIPER-TIMING-NOTFNS-MIB** table. PR1439025
- The ports of the EX devices might stay in the **Up** state even if the EX4600 or QFX5100 lines of switches is rebooted. PR1441035
- The interface might go into the **Down** state after the FPC restarts with the PTP configuration enabled. PR1442665
- The BGP session fails to establish when you use the firewall filter to de-encapsulate BGP packets from the GRE tunnel. PR1443238
- System reboot is required when GRES is enabled or disabled with the **mobile-edge** configuration. PR1444406
- Irregular traffic drop might be seen when the traffic is ingress from MPC3E and egress to MPC10E. PR1445649
- When you use a converged CPCD, an MX Series router rewrites the HTTPS request with the destination-port 80. PR1446085
- When switchover happens with an MX Series router with service interface that has NAT and GR configuration, the static route for NAT never comes up. PR1446267
- DT_BNG: bbe-smgd generates core file on the backup Routing Engine in **bbe_ifd_add_vlan (ifd=0x8c3e835, ifl=0xcaf59f18)** at **../../../../../../src/junos/usr.sbin/bbe-svcs/smd/infra/bbe_ifd.c:6374**. PR1447493
- IPv6 throughput numbers for NAT with HTTP traffic are not at par with IPv4. PR1449435
- Changing the hostname triggers the LSP on-change notification and not the adjacency on-change notification. PR1449837
- On the MPC10E line card, dcd is unable to clean stale the mt- logical interfaces while reloading rosen configuration on the DUT. PR1450953

- When you use the Standard_D5_v2, which has 16 vCPUs and 56 GB of memory, the deployment fails. PR1450975
- JNP10000-LC2101 FPC generates **Voltage Tolerance Exceeded** major alarm for each IP 2V5 sensor. PR1451011
- Main chassisd thread at the JNS GNF might stall upon the GNF SNMP polling for hardware-related OIDs. PR1451215
- Need to add support for drop flows when the packet drops. PR1451921
- On the MX10000 and PTX10000 lines of routers with Routing Engine redundancy configuration enabled, the firmware upgrade for PSU (JNP10000-AC2) and JNP10000-DC2) might fail due to lcmd being disabled by the firmware upgrade command. PR1452324
- Sensord core file might be seen when the script runs on MPC10E line card. PR1452976
- On an MPC10E line card, inconsistency between AFT and non-AFT line cards occurs while displaying ldp p2mp traffic-statistics on the bud node. PR1453130
- Add the **syslog** configuration command to the stateful firewall rule then condition. PR1453502
- On an MX10003 device, alarms are not sent to syslog. PR1453533
- The VMX might work abnormally in a large topology. PR1453967
- The 100-Gigabit Ethernet interfaces might not come up again after going down on MPC3E-NG. PR1454595
- When the scale configurations are applied, chassisd CLI command might delay response or might time out for 10 minutes. PR1454638
- On the line card, interface damping is not supported. PR1455152
- The smihelperd process is not initialized when Junos OS is upgraded on PPC-based platforms. PR1455667
- Multiple daemons might crash on committing configuration changes related to groups. PR1455960
- Along with the 4x1GE feature using the QSFP28 optics, continuous logging in the chassisd file is observed when speed 1-Gigabit Ethernet is configured with **pic_get_nports_inst** and **ch_fru_db_key**. PR1456253
- On the line card, need to add the support of optics-options low light. PR1456894
- The bbe-statsd process might continuously crash if any parameter is set to 0 in the **mx_large.xml** file. PR1457257
- On the JSU package installed for lcmd, the daemon might not restart the daemon with the new daemon package. PR1457304
- The chassisd process and all FPCs might restart after Routing Engine switchover. PR1457657
- After more than 2 million multicast subscribers are activated without performing GRES or bbe-smgd restart, further multicast subscribers might be unable to log in. PR1458419

- Traffic silently discards or MPC crashes on the MPC10E line card during the change of the firewall filter terms. PR1458499
- If you use the dynamic VoIP VLAN assignment, the correct VoIP VLAN information in LLDP-MED packets might not be sent after you commit. PR1458559
- The FPC X major errors alarm might be raised after committing the PTP configuration change. PR1458581
- The rpd crash might be seen if the BGP route is resolved over the same prefix protocol next hop in the inet.3 table that has both the RSVP and LDP routes. PR1458595
- The traffic might be stuck on MS-MPC or MS-MIC with sessions receiving a huge number of affinity packets. PR1459306
- The following error message might be seen after the chassisd restarts: **create_pseudos: unable to create interface device for pip0 (File exists).** PR1459373
- The **show ancp subscriber access-aggregation-circuit-id < access aggregation circuit ID>** command displays incomplete output. PR1459386
- Telemetry streaming of mandatory TLV ttl learned from LLDP neighbor is missing. PR1459441
- The traffic might be silently dropped or discarded during the link recovery in an open Ethernet access ring with ERPS configured. PR1459446
- Inline S-BFD packets are dropped on MPC6E MIC1/PIC1 ports: 0-11. PR1459529
- In an MC-LAG scenario, the traffic destined to VRRP-virtual MAC gets dropped. PR1459692
- After the DRD auto-recovery, the traffic is silently dropped or discarded during interface flaps. PR1459698
- Configuration change might not be applied if the Ephemeral database is used. PR1459839
- Initial synchronization for the **OpenConfig** event sensors are streamed only from producers supporting event paths. PR1459927
- On the line card, interface flaps multiple times after an administrator disables or enables at the side or when an optical module is plugged into. PR1459942
- In a subscriber management environment, subscriber statistics reported by CLI commands and RADIUS can be broken if ISSU is performed from any Junos OS Release earlier than 18.4 to 18.4 or later. PR1459961
- The PPTP does not work with destination NAT. PR1460027
- If **vlan-offload** is configured on the VMX platform, **input-vlan-map** might not work. PR1460544
- Support of **del_path** for the LLDP neighbor changes at various levels. PR1460621
- When you receive IPv6 over IPv4 IBGP session, the IPv6 prefix is hidden. PR1460786
- The PTP function might consume the kernel CPU for a long time. PR1461031
- Explicit Deletion Notification (del_path) are not received when the LLDP neighbor is lost as result of disabling the local interface on the DuT through CLI (gNMI). PR1461236

- The bbe-smgd generates a core file when all RADIUS servers are unreachable. PR1461340
- Traffic might be impacted due to fabric hardening being stuck. PR1461356
- The traffic might not be forwarded when it is received from the circuit cross-connect interface. PR1461532
- On the MPC10E line card, more output packets are seen than expected when the ping function is performed. PR1461593
- In an EVPN scenario, memory leak might be observed when **proxy-macip-advertisement** is configured. PR1461677
- The repd generates a core file during system startup. PR1461796
- During the BBE statistics collection and management process, issues with the bbe-statsd memory on the backup Routing Engine occur. PR1461821
- JET RIB API RouteRemove and RouteRemoveMatching RPCs do not work as the first RIB API call. PR1461974
- The rpd might crash after committing the **dynamic-tunnel-anchor-pfe** command. PR1461980
- The rpd process might crash if the **show v4ov6-tunnels information anti-spoof-ip** command is executed. PR1462047
- The following error message appears when both the DIP switches and power switch are turned off: **CHASSISD_SNMP_TRAP6: SNMP trap generated: Power Supply failed.** PR1462065
- The flow stuck and flowd watchdog generate core files while trying to ping the DNS server 8.8.8.8 on the internet through DUT configured with NAPT44. PR1462277
- Traffic drops over the aggregated Ethernet interfaces configured with Virtual Router Redundancy Protocol (VRRP). PR1462310
- On an MX204 router, the RADIUS interim accounting statistics are not populated. PR1462325
- The EA WAN SerDes gets into the **Stuck** state that leads to continuous **DFE tuning timeout** errors and causes the link to stay down. PR1463015
- The vty remote MAC addresses are not learned with correct age if vty is from a line card without Juniper Trio 5 silicon. PR1463040
- MAC-learning is broken for vlan-id all scenario. PR1463078
- The Routing Engine switchover might not be triggered when the master CB clock fails. PR1463169
- MVPN traffic might be dropped after performing switchover. PR1463302
- The subscribers might not pass traffic after making some changes to the dynamic-profiles filter. PR1463420
- RPC ALG causes MSPMAND to generate core files when an MX Series router is used as a stateful firewall with the MS-MIC or MS-MPC service cards. PR1464020

- The IPoE subscriber route installation might fail. PR1464344
- Observing **bbe-smgd-core (0x000000000088488c** in **bbe_autoconf_delete_vlan_session_only (session_id=918)** at **../../../../../../src/junos/usr.sbin/bbe-svcs/smd/plugins/autoconf/bbe_autoconf_plugin.c:3115)**. PR1464371
- The PPP IPv6CP might fail if the **routing-services** command is enabled. PR1464415
- The CPU utilization on mgd daemon might get stuck at 100 percent after the netconf session is interrupted by flapping interface. PR1464439
- The MS-MIC might not work when it is used on a specific MPC. PR1464477
- The **show task memory detail** command shows incorrect cookie information. PR1464659
- The PPPoE session goes in to the **Terminated** state and the accounting stops for the session that is delayed. PR1464804
- MPC5E or MPC6E might crash due to internal thread hogging of the CPU. PR1464820
- The end in front of NAT also sends NATT keep alive packets. PR1464864
- Commit script does not apply changes in the private mode unless a commit full is performed. PR1465171
- The jdhcpd might consume high CPU and no further subscribers can be brought up if more than 4000 dhcp-relay clients are present in the MAC-MOVE scenario. PR1465277
- The physical interface of aggregated Ethernet might take time to come up after disabling or enabling the interface. PR1465302
- Bandwidth percent with shaping rate does not work on an aggregated Ethernet interface after deactivating and activating the class of service. PR1465766
- ICMP error messages does not appear even enabling the **enable-asymmetric-traffic-processing** statement. PR1466135
- The PPPoE subscribers get stuck due to the PPPoE inline keepalives that do not work properly. PR1467125
- Layer 2 wholesale does not forward all the client requests with stacked VLAN. PR1467468
- Hot-swapping between MPC11E and legacy MPC9, MPC8, or MPC6 is not supported. PR1467725
- The process rpd might crash after making several changes to the flow-spec routes. PR1467838
- Crypto code might cause high CPU utilization. PR1467874
- You might observe the following error message: **the user-ad-authentication subsystem is not responding to management requests**. PR1467991
- The **satellite-management** commands are not available. PR1467997
- Benign logs might show in Junos OS Release 19.3R2 when switching between configurations using **load-override** with GRES and **commit-synchronize**. PR1468234

- Optics measurements might not be streamed for the interfaces of a PIC over JTI. PR1468435
- The process rpd crash might be seen if the BGP sharing is enabled. PR1468676
- The **Inner-list** functionality with dual tag does not work. Traffic gets dropped at the ingress port. PR1469396
- The tcp-log connections fail to reconnect and get stuck in the **Reconnect-In-Progress** state. PR1469575
- Memory leak on Layer 2 cpd process causes Layer 2 cpd to crash. PR1469635
- A hierarchical-scheduler should not be configured on a ps- interface. PR1470049
- On the MPC11E line card, some of the 10-Gigabit Ethernet interface states might not get cleaned up correctly when performing GRES with invalid profile configuration. PR1470153
- On MPC-11E interfaces, certain configuration steps might cause traffic to not get policed properly. PR1470629
- The SNMP interface-mib stops working for the PPPoE clients. PR1470664
- On MPC11E, PIC online event does not generate SNMP trap when PIC goes through offline to online transition. PR1470796
- Unable to setup 26M sessions (NAPT44) at 900,000pps per second. PR1470833
- On rare occasions, the router might send out one extra URR quota value for a bearer. PR1470890
- Sudden FPC shutdown due to hardware failure or ungraceful removal of line card might cause major alarms on other FPCs in the system. PR1471372
- In the cRPD platform, license violations are captured as nagging log messages and no alarm is raised. PR1471455
- The clksyncd crash might be seen when PTP over an aggregated Ethernet interface is configured on the MX104 platform. PR1471466
- Phase or frequency synchronization might not work correctly when PTP is configured in the hybrid mode. PR1471502
- MTU errors count captured in the **show pfe statistics traffic** does not match exactly to the actual count of the frames dropped. PR1471554
- On the MX10008 and MX10016 line cards, the ARP suppression (default enabled) in EVPN does not work. PR1471679
- PCC tries to send a report to PCE but the connection between PCC and PCE is not in the **Up** state especially in the case of MBB in PCE provisioned or controlled LSP. PR1472051
- On multicore next-generation Routing Engines on the MX960, MX240, and MX480 routers with USF mode enabled and USF-based services configuration, the subsequent Junos vmhost upgrade fails with an error message. PR1472287
- Chassis alarm on BSYS might be observed : **RE0 to one or many FPCs is via em1: Backup RE.** PR1472313

- Service accounting statistics do not get updated after changes are made to the firewall filters. PR1472334
- The kernel might crash and vmcore might be observed after the configuration change is committed. PR1472519
- Performing back-to-back rpd restarts might cause rpd to crash. PR1472643
- Active error counts do not increase for I2C in the synchronization cards. PR1472660
- On the MX Series devices, if the **reauthenticate lease-renewal** statement is enabled for DHCP, when the DHCP authentication and re-authenticate lease-renewal occurs, the SDB might go down very frequently. PR1473063
- Drops counter does not increment for the aggregated Ethernet even after the member link shows the drops. PR1473665
- Ingress multicast replication does not work with the GRES configuration. PR1474094
- An MPC11 crash might occur on the MX2000 platform using multi dimensional advanced scale configuration that has inline keep alive sessions. PR1474160
- MX10000 QSA adapter lane 0 port goes in the **Down** state when you disable one of the other lanes. PR1474231
- With URR enabled, the URR reports cause memory leak. Eventually, the heap memory gets exhausted. PR1474306
- The **show services sessions** and **show services sessions extensive output** commands do not display the member interface of the AMS where the session got landed. They display only the AMS interface name. PR1474313
- When traffic loss is observed on a 100-Gigabit Ethernet logical interface, the MACsec sessions are up and live. PR1474714
- The **request system power-off** and **request system halt** commands might not work correctly. PR1474985
- The clksyncd generates core files after GRES. PR1474987
- SFW rule configuration deletion might lead to memory leakage. PR1475220
- The Radius accounting updates of the service session have incorrect statistic data . PR1475729
- Dark window size is more than expected and 31.0872721524375 seconds of traffic loss is observed. PR1476505
- The bbe-mibd might crash on the MX Series platform in a subscriber environment. PR1476596
- The MX Series router acting as LNS does not get to program the Packet Forwarding Engine with l2tp services, which causes forwarding issues for the l2tp subscribers. PR1476786
- Traffic loss might be seen in the SAEGW scenario after the daemon restarts or after the GRES operation. PR1477461
- IKE version 2 tunnel flaps with DPD occur if initiator is not behind NAT. PR1477483

- The Packet Forwarding Engine might be disabled due to major errors on MPC2E-NG, MPC3E-NG, MPC5, MPC6, MPC7, MPC8, and MPC9 line cards. PR1478028
- The **show evpn statistics instance** command gets stuck on the multihomed scenario. PR1478157
- At scale log ins of both the default and dedicated bearers might require retries from the control plane. PR1478191
- FPC memory leak might happen after executing the **show pfe route** command. PR1478279
- [firewall] [filter_installation] Output chain filter counters are not correct. PR1478358
- The core files are generated at **cassis_alloc_list_timed_free in cassis_free_thread_entry**. PR1478392
- The protocol MTU might not be changed on the lt- interface from the default value. PR1478822
- The TCP-log sessions might be in the **Established** state but no logs get sent out to the syslog server. PR1478972
- The rpd process might crash when executing the **show route protocol l2-learned-host-routing** or **show route protocol rift** command on a router. PR1481953
- The MX204 router reboots when the PPPoE client starts to log in and no core files are generated. PR1482431
- Packet loss might be observed after the device reboots or l2ald restarts in an EVPN-MPLS scenario. PR1484468
- UID might not be released properly in some scenarios after the service session deactivation. PR1188434
- The **show subscriber extensive** command incorrectly displays DNS address provided to the DHCP clients. PR1457949
- PPP IPv6 NCP fails to negotiate during the PPP login. PR1468414
- DHCP relay with forward-only fails to send OFFER when the client is terminated on the lt-0/0/0.2 logical tunnel interface. PR1471161
- Dynamic-profile for VPLS-PW pseudowire incorrectly reports the Dynamic Static Subscriber Base Feature license alarm. PR1473412
- DHCP-server RADIUS given mask is being reversed. PR1474097

Infrastructure

- The kernel crashes during the removal of the mounted USB when a file is being copied to it. PR1425608
- Slow response from SNMP might be observed after an upgrade to Junos OS Release 19.2R1. PR1462986
- The scheduled tasks might not be executed if the cron daemon goes down without restarting automatically. PR1463802

Interfaces and Chassis

- Restarting chassisd with GRES disabled might cause FPC to restart and some demux interfaces to be deleted. PR1337069
- When the logical interface is associated to a routing-instance inside a LR, the logical interface is removed from the routing-instance and the logical interface is not added to the default routing instance. PR1444131
- Continuous VRRP state transition (VRRP master or backup flaps) is observed when one device drops the VRRP packets. PR1446390
- Interface descriptions might be missing under the logical systems CLI. PR1449673
- Mismatched MTU value causes the RLT interface to flap. PR1457460
- The EOAM CFM primary-vid functionality does not work if the **enhanced-cfm-mode** is enabled. PR1465608
- vrrpv3mibs does not work on the QFX platform to poll the VRRPv6 related objects. PR1467649
- The voltage high alarm might not be cleared when voltage level comes back to normal for MIC on MPC5. PR1467712
- When you configure ESI on a physical interface, the traffic drops when you disable the logical interface under the physical interface. PR1467855
- When dynamic DHCP sessions exist in the device and if multiple commits in parallel are performed, the commit might become nonresponsive. PR1470622
- Commit error was not thrown when the member link was added to multiple aggregation groups with different interface specific options. PR1475634
- When the addition and the deletion of an logical interface (both logical interfaces with the same VLAN ID) is performed in a single commit configuration, the check fails with the following error message: **duplicate VLAN-ID.** PR1477060
- MC-AE interface might be shown as an unknown status when you add the sub interface as part of the VLAN on the peer MC-AE node. PR1479012
- For ATM interfaces configuration, if any logical interface has the **allow-any-vci** configuration, then the commit operation might fail. PR1479153

Junos Fusion Enterprise

- Loop detection might not work on the extended ports in the Junos fusion scenarios. PR1460209

Layer 2 Ethernet Services

- The jdhcpd process might go into infinite loop and cause CPU full utilization. PR1442222
- DHCP subscriber might not come online after the router reboots. PR1458150
- On the MX2010 and MX2020 lines of routers, no alarm is generated when FPC is connected to the master Routing Engine through the backup Routing Engine. PR1461387
- The metric does not change when configured under DHCP. PR1461571
- Member links state might be asynchronized on a connection between PE and CE devices in the EVPN A/A scenario. PR1463791
- The ISSU might fail during the subscriber in-flight login. PR1465964
- Telemetry data for **relay/bindings/binding-state-v4relay-binding** and **relay/bindings/binding-state-v4relay-bound** are not correct. PR1475248

MPLS

- The FPC might be stuck in the **Ready** state after making a change in the configuration that removes RSVP and triggers FPC restart. PR1359087
- On the MPC10E or MPC11E line card, the LDP and BFD sessions are dropped when the **fast-lookup-filter** has a default term with only accept as action and it is attached to the lo0 interface. PR1474204
- The root XML tag in the output is changed from **rsvp-pop-and-fwd-info** to **rsvp-pop-and-fwd-information** to be consistent with the XML tag convention. PR1365940
- Traffic is silently discarded after the LSP protection link on the third-party transit router goes down. PR1439251
- On the MPC10E line card, the P2MP LSP traceroute is not working. PR1440636
- The traffic might be silently discarded after the LACP times out. PR1452866
- P2MP LSP might flap after the VT interface in the MVPN routing instance is reconfigured. PR1454987
- The rpd core files are generated with SNMP polling. PR1457681
- All LDP adjacencies flap after changing LDP preference. PR1459301
- The previously configured credibility preference is not considered by CSPF even though the configuration has been deleted or changed to prefer another protocol in the traffic engineering database. PR1460283
- MPLS trace route does not trace the SRUDP tunnel ingress router. PR1460516

- The process rpdtmd might crash while SNMP polls the statistics of the lpd interface. PR1465729
- The device might use the locally computed path for the PCE-controlled LSPs after the link or node fails. PR1465902
- The fast reroute detour next-hop down event might cause the primary LSP to go in the **Down** state in a particular scenario. PR1469567
- The p2mp traceroute fails with an aggregated Ethernet bundle over AFT. PR1470815
- The rpd process might crash during shutdown. PR1471191
- The rpd crash might be seen after some commit operations, which might affect the RSVP ingress routes. PR1471281
- The following error messages continuously floods the backup Routing Engine: **(JTASK_IO_CONNECT_FAILED: RPDTM./var/run/rpdtmd_control: Connecting to 128.0,255.255,255.255,0.0.0.0,0.0.0.0, failed: No such file or directory).** PR1473846
- RSVP LSPs might not come up in the scaled network with a very high number of LSPs if NSR is used on the transit router. PR1476773
- Kernel crashes and device might restart. PR1478806
- The rpd process crashes on the backup Routing Engine when LDP tries to create LDP p2mp tunnel upon receiving corrupted data from the master Routing Engine. PR1479249

Network Management and Monitoring

- The SNMP cold start trap might be seen after the Routing Engine switchover. PR1461839

Platform and Infrastructure

- The jcrypto syslog help package and events are not packaged even when the error message is compiled. PR1290089
- The time convergence for the MVPN fast upstream failover might be more than 50 minutes. PR1478981
- With chained composite next-hop enabled, the MPLS CoS rewrite does not work for IPv6 PE device traffic. PR1436872
- In an EVPN-VXLAN scenario, sometimes the host-generated packets get dropped when hitting the reject route in the Packet Forwarding Engine. PR1451559
- The MPC might drop packets after enabling the firewall fast lookup filter. PR1454257
- Multicast traffic loss occurs in a rare case in a seamless MPLS with MVPN configuration. PR1456905
- Port mirroring does not occur with VPLS. PR1458856
- DDoS-protection does not stop logging when the remote tracing is enabled. PR1459605

- Traceroute initiated from the PE device does not show the tunnel endpoint hop in the output. PR1461441
- CLI configuration flag **version-03** must be optional. PR1462186
- On the MX204 platform, Packet Forwarding Engine errors might occur when the incoming GRE tunnel fragments get sampled and undergo inline reassembly. PR1463718
- Not able to view the snapshots of the backup Routing Engine. PR1464394
- MX80 EVPN-VXLAN RT5 does not work properly, and **ip-prefix-routes** are not reachable. PR1466602
- On the MX150 devices, the default subscriber management license does not include the Layer 2 TP. PR1467368
- On the MX Series Virtual Chassis, the Layer 2 traffic sent from one member to another member is corrupted. PR1467764
- The JNH memory leaks after the CFM session flap for the LSI and VT interfaces. PR1468663

Routing Policy and Firewall Filters

- Routes resolution might be inconsistent if any route resolves over the multipath route. PR1453439

Routing Protocols

- The CPU utilization on rpd spins at 100 percent once the same external BGP route is learned on different VRF tables. PR1442902
- If the same neighbor is configured under different RIP groups, the commit check fails to capture this invalid configuration and commit is done successfully. However, the rpd process crashes. PR1485009
- The rpd crash might be seen after configuring OSPF **nssa area-range** and summaries. PR1444728
- The BGP routes might fail to be installed in a routing instance if the **from next-hop** policy match condition is used in the VRF import policy. PR1449458
- TI-LFA backup path for the adj-sids is broken in OSPF, where the shortest path to the node opposite the adj-sid is not the one-hop path over the interface indicated by the adj-sid. PR1452118
- The SSH login might fail if a user account exists in both the local database and RADIUS/TACACS+. PR1454177
- The rpd scheduler slip for BGP GR might be up to 120 seconds after the peer goes down. PR1454198
- MoFRR with MLDP inband signaling is not working. PR1454199
- The rpd memory might leak in certain MSDP scenario. PR1454244
- The rpd might crash continuously due to memory corruption in the IS-IS setup. PR1455432
- Packet drop and CPU spike on the Routing Engine might be seen in certain conditions if **labeled-unicast protection** is enabled for a CsC-VRF peer. PR1456260

- The topology-independent loop-free alternate might be unable to install backup path in the routing table in a specific case. PR1458791
- The rpd memory leak might be observed on the backup Routing Engine due to BGP flap. PR1459384
- The other querier present interval timer cannot be changed in a IGMP or MLD snooping scenario. PR1461590
- The rpd scheduler slips might be seen on the RPKI route validation enabled BGP peering router in a scaled setup. PR1461602
- Need to install all possible next hops for the OSPF network LSAs. PR1463535
- The IS-IS IPv6 multitopology routes might flap every time when there is an unrelated commit under the protocol statement. PR1463650
- The rpd might crash if both the BGP add-path and BGP multipath are enabled. PR1463673
- The rpd might crash if the IPv4 routes are programmed with the IPv6 next hop via JET APIs. PR1465190
- The BGP peers might flap if the **hold-time** parameter is set as small. PR1466709
- The configured BGP damping policy might not take effect after BGP is disabled and then enabled followed by commit. PR1466734
- BGP multipath does not work for MT on cRPD. PR1467091
- The rpd might crash after configuring **independent-domain** under the master routing instance. PR1469317
- The mcsnoopd might crash when the STP moves the mrouter port to the **Blocked** state. PR1470183
- The BFD client session might flap when removing the BFD configuration from the peer end (from other vendor) of the BFD session. PR1470603
- The rpd might crash when both the **instance-import** and **instance-export** policies contain the **as-path-prepend** action. PR1471968
- The rpd process might crash with the BGP multipath and damping configured. PR1472671
- Removal of the cluster from the BGP group might cause prolonged convergence times. PR1473351
- SFTP does not connect properly and the following error message is seen**: Received message too long.** PR1475255
- The rpd process might crash with BGP multipath and route withdrawal occasionally. PR1481589
- Removal of the BGP and rib-sharding configuration might cause the routing protocols to become unresponsive. PR1485720
- High CPU utilization might be observed when the outgoing BGP updates are sent slowly. PR1487691

Services Applications

- The jl2tpd process might crash during the restart procedure. PR1461335
- The calling station gets truncated after 64 bytes. PR1462689
- On an MX Series router, L2tp LTS fails to forward the **agentCircuitId** and **agentRemoteId** AVP toward the LNS. PR1472775
- Phase 1 SA migrates to a new remote IP because of the **source-address translation** for the static NAT tunnel. PR1477181

Subscriber Access Management

- The authd crashes on the backup Routing Engine during execution of the slax script that runs the **< get-jsrc-counters>** RPC call. PR1458185
- DHCPv6 subscribers might be stuck in a state after the authd process crashes. PR1460578
- A problem arises with **linked-pool-aggregation** after attempting to delete a pool in the middle of the chain. PR1465253
- The volume statistics attributes are missing in the accounting-stop for the Configuration Activated Services and CLI Activated Services. PR1470434
- The sub interfaces might be missing in the NAS port ID. PR1472045
- The authd process might crash after the ISSU setup from Junos OS Release 18.3 and earlier to Junos OS Release 18.4 and later. PR1473159
- Some address-relevant fields are missing when executing the **test aaa ppp** command. PR1474180
- The CoA request might not be processed if it includes the **proxy-state** attribute. PR1479697
- The **mac-address** CLI option is hidden under the **access profile radius options calling-station-id-format** statement. PR1480119

User Interface and Configuration

- On an MX Series device, a J-Web page might not get redirected to login once the session expires with an idle timeout. PR1459888

VPNs

- The P1 configuration delete message is not sent on loading baseline configuration if there has been a prior change in VPN configuration. PR1432434
- The rpd process might crash due to memory leak in MVPN RPF Src PE block. PR1460625

- The Layer 2 circuit displays MM status, which might cause traffic loss. PR1462583
- The Layer 2 circuit connections might become stuck in the **OL** state after changing the Layer 2 circuit community and flapping the primary LSP path. PR1464194
- The rpd might crash when **link-protection** is added or deleted from LSP for the MVPN ingress replication selective provider tunnel. PR1469028

SEE ALSO

What's New | **71**

What's Changed | **103**

Known Limitations | **105**

Open Issues | **108**

Documentation Updates | **133**

Migration, Upgrade, and Downgrade Instructions | **134**

Documentation Updates

IN THIS SECTION

This section lists the errata and changes in Junos OS Release 20.1R1 documentation for the MX Series.

Dynamic Host Configuration Protocol (DHCP)

- **Introducing DHCP User Guide**—Starting in Junos OS Release 20.1R1, we are introducing the DHCP User Guide for Junos OS routing, switching, and security platforms. This guide provides basic configuration details for your Junos OS device as DHCP Server, DHCP client, and DHCP relay agent.

  [See DHCP User Guide.]

SEE ALSO

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 17.4R1 release, FreeBSD 11.x is the underlying OS for all Junos OS platforms which were previously running on FreeBSD 10.x based Junos OS. FreeBSD 11.x does not introduce any new Junos OS related modifications or features but is the latest version of FreeBSD.

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

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

Basic Procedure for Upgrading to Release 20.1R1

> **NOTE:** Before upgrading, back up the file system and the currently active Junos OS configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. Issue the following command:
>
> ```
> user@host> request system snapshot
> ```
>
> The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the **juniper.conf** and **ssh** files) might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see the Installation and Upgrade Guide.

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

Procedure to Upgrade to FreeBSD 11.x based Junos OS

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

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

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

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

2. Select the name of the Junos OS platform for the software that you want to download.

3. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.

4. Select the **Software** tab.

5. In the **Install Package** section of the **Software** tab, select the software package for the release.

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

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

10. Install the new **jinstall** package on the routing platform.

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

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

- For 32-bit Routing Engine version:

  ```
  user@host> request system software add no-validate reboot
  source/junos-install-mx-x86-32-20.1R1.9-signed.tgz
  ```

- For 64-bit Routing Engine version:

  ```
  user@host> request system software add no-validate reboot
  source/junos-install-mx-x86-64-20.1R1.9-signed.tgz
  ```

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

- For 32-bit Routing Engine version:

  ```
  user@host> request system software add no-validate reboot
  source/junos-install-mx-x86-32-20.1R1.x-limited.tgz
  ```

- For 64-bit Routing Engine version:

  ```
  user@host> request system software add no-validate reboot
  source/junos-install-mx-x86-64-20.1R1.9-limited.tgz
  ```

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

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

- **http://*hostname/pathname***
- **scp://*hostname/pathname***

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

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

Rebooting occurs only if the upgrade is successful.

NOTE:

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the **request vmhost software add** command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.
- Starting in Junos OS Release 20.1R1, 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 20.1R1 **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-20.1R1.9-signed.tgz**

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

```
user@host> request system software add validate reboot
source/jinstall-ppc-20.1R1.9-limited-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

> **NOTE:** After you install a Junos OS Release 20.1R1 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before

or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

Upgrading a Router with Redundant Routing Engines

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

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

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

Downgrading from Release 20.1R1

To downgrade from Release 20.1R1 to another supported release, follow the procedure for upgrading, but replace the 20.1R1 jinstall package with one that corresponds to the appropriate release.

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

For more information, see the Installation and Upgrade Guide.

SEE ALSO

- What's New | 71
- What's Changed | 103
- Known Limitations | 105
- Resolved Issues | 115
- Open Issues | 108

Junos OS Release Notes for NFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 20.1R1 for the NFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

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

Application Security

- **AppQoE support for granular APBR rules (NFX Seris, SRX Series, and vSRX)**—Starting in Junos OS Release 20.1R1, AppQoE utilizes the granular rule matching functionality of advanced policy-based routing (APBR) for better quality of experience (QoE) for the application traffic.

  In Junos OS Release 18.2R1, APBR supported configuring policies by defining source addresses, destination addresses, and applications as match conditions. After a successful match, the configured APBR profile is applied as an application services for the session. In this release, AppQoE leverages the APBR enhancement and selects the best possible link for the application traffic as sent by APBR to meet the performance requirements specified in SLA.

  [See Application Quality of Experience.]

- **Default mechanism to forward the traffic through APBR rule (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS 20.1R1, you can configure a APBR rule by specifying the dynamic application match criteria with any keyword. This provides a default mechanism to forward the traffic to a specific next-hop device or to a destination if the traffic matches any dynamic application.

  [See Advanced Policy-Based Routing.]

- **Custom application enhancements (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 20.1R1, we've enhanced the custom applications signature functionality by providing a new set of applications and contexts.

  Application identification allows you to create custom application signatures to detect applications specific to your network environment. You can create custom application signatures for applications based on ICMP, IP protocol, IP address, and Layer 7 or TCP/UDP stream. While configuring the custom application signatures, you must specify the context values that the device can use to match the patterns in the application traffic.

  Custom application signature contexts are part of application signature package. You must download and install the latest application signature package version 3248 or later to use new contexts for custom application signatures.

  [See Custom Application Signatures for Application Identification.]

Interfaces

- **Single-leg and unidirectional cross-connect**— Starting in Junos OS Release 20.1R1, NFX Series devices support single-leg cross-connect and unidirectional cross-connect features.

  Single-leg cross-connect feature allows configuration of single entry in the cross-connect. The entry can be either VNF interface or a virtual interface. You can configure the other entry in the cross-connect at any later point of time.

  Unidirectional cross-connect feature allows the traffic to be forwarded conditionally or unconditionally in a single direction. Traffic flow in the opposite (other) direction follows the MAC-based forwarding rule.

  [See How to Configure NFX150, How to Configure NFX250, and How to Configure NFX350.]

Virtualized Network Functions (VNFs)

- **Virtual router reflector (VRR) virtualized network function (VNF) in enhanced orchestration (EO) mode**— Starting in Junos OS Release 20.1R1, you can instantiate the VRR VNF in EO mode by using the JDM CLI configuration and without using the XML descriptor file. EO mode uses Open vSwitch (OVS) as an NFV backplane for bridging the interfaces.

  [See Managing Virtual Network Functions Using JDM.]

SEE ALSO

What's Changed

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

SEE ALSO

Known Limitations

There are no known limitations for NFX Series devices in Junos OS Release 20.1R1.

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

SEE ALSO

What's New | 141
What's Changed | 143
Open Issues | 144
Resolved Issues | 146
Documentation Updates | 148
Migration, Upgrade, and Downgrade Instructions | 148

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 20.1R1 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 issue a **show interface** command on NFX150 devices 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
- On NFX150 and NFX250 NextGen devices, when you add, modify, or delete a VNF interface that is mapped to an L2 or L3 data plane, kernel traces might be observed on the NFX Series device console. PR1435361
- The heth-0-4 and heth-0-5 ports do not detect traffic when you try to activate the ports by plugging or unplugging the cable. As a workaround, perform a link flap or enable or disable the interface using the CLI. PR1449278

Platform and Infrastructure

- Jumbo frames are not supported through OVS on an NFX250 device. PR1420630
- On an NFX250-LS1 device that is operating in Compute mode, the traffic throughput rate is be reduced with OVS cross-connect configuration. PR1438687
- On an NFX Series device, an srxpfe core file might be seen when you attempt to configure, reconfigure, or delete the dual VF mappings on the device. PR1458452

SEE ALSO

What's New | **141**

What's Changed | **143**

Known Limitations | **144**

Resolved Issues | **146**

Documentation Updates | **148**

Migration, Upgrade, and Downgrade Instructions | **148**

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS Release 20.1R1 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.

High Availability

- On an NFX150 high availability chassis cluster, the host logs updated in the system log messages might not show the correct time stamp. PR1394778

Interfaces

- On NFX150 devices, no error is displayed when the commit fails after you configure **native-vlan-id** on an access VNF interface. PR1438854
- On NFX Series devices, ping is not working between the cross-connected interfaces with interface deny-forwarding configuration. PR1442173
- On NFX Series devices, the static MAC address is replaced by a random MAC address. PR1458554
- When traffic goes through vSRX3.0 platforms, core-dump files are generated and traffic is dropped. This issue might result in the Packet Forwarding Engine being inactive and all interfaces being down. PR1465132
- On NFX150 devices, GRE tunnel interface (gr-1/0/0) might not appear if the **clear-dont-fragment-bit** option is configured for the GRE interface. PR1472029
- On NFX350 devices, if you delete and add SXE interfaces, the SXE interface moves to Spanning Tree Protocol blocking (STP BLK) state, and the traffic drops on that interface. PR1475854

Mapping of Address and Port with Encapsulation (MAP-E)

- On NFX Series devices, IP identification (IP ID) is not changed after MAP-E NAT44 is performed on fragment packets when the packets reach the customer edge (CE) device.

  PR1478037

Platform and Infrastructure

- LTE package related files are lost after image upgrade from Junos OS Release D497.1 to Junos OS Release 18.4R3.3 on NFX250 devices. PR1493711
- On NFX Series devices, if there are any conditional groups, the l2cpd process might crash and generate a core dump when interfaces are flapping and the LLDP neighbors are available. It might cause the dot1x process to fail and all the ports have a short interruption at the time of process crash. PR1431355
- Half-duplex configuration on 1-Gigabit Ethernet ports is not supported when auto negotiation is disabled. PR1453911
- On NFX350 devices, if you execute the **show vmhost mode** command multiple times, JDM might crash and cause the **show vmhost mode** commands to stop working. PR1474220
- After a power outage, JDMD is not responsive because the **/etc/hosts** file is corrupted on NFX250 devices. PR1477151

Routing Protocols

- On NFX Series devices, changing the **other querier present interval** timer is not working on IGMP or the MLD snooping device in the existing bridge domain (BD) or listener domain (LD). PR1461590

Virtualized Network Functions (VNFs)

- On NFX150 and NFX250 NextGen devices, when two flowd interfaces are mapped to the same physical interface and if you delete the interface mapping to VF0, the traffic flow is disrupted. Even though the mapping is moved to VF0, the MAC address is not cleared in VF1, which disrupts the traffic. PR1448595
- On NFX150 devices, when you need to change the vmhost mappings of a particular NIC or NICs, you must delete the existing vmhost mapping and commit the configuration. Now you can configure the new mappings for the respective NICs. You cannot change the NIC vmhost mappings in the same commit to delete and add a new mapping to the heth NICs. PR1459885
- NFX250 devices do not allow *jdm* (case-insensitive) as a VNF name. You can use *jdm* as a part of the name. For example, *jdm123*, *abcJDM*, *abcJDM123* are valid VNF names, whereas, *jdm*, *JDM*, *Jdm*, *JDm* are not valid VNF names. PR1463963

SEE ALSO

- What's New | 141
- What's Changed | 143
- Known Limitations | 144
- Open Issues | 144
- Documentation Updates | 148
- Migration, Upgrade, and Downgrade Instructions | 148

Documentation Updates

There are no errata or changes in Junos OS Release 20.1R1 documentation for NFX Series.

SEE ALSO

- What's New | 141
- What's Changed | 143
- Known Limitations | 144
- Open Issues | 144
- Resolved Issues | 146
- Migration, Upgrade, and Downgrade Instructions | 148

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.

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 20.1

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

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

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

To download and install Junos OS Release 20.1R1:

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

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

2. Select the name of the Junos OS platform for the software that you want to download.

3. Select the **Software** tab.

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

5. In the Install Package section of the Software tab, select the software package for the release.

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

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

9. Copy the software to the device or to your internal software distribution site.

10. Install the new package on the device.

SEE ALSO

What's New | **141**

What's Changed | **143**

Known Limitations | **144**

Open Issues | **144**

Resolved Issues | **146**

Documentation Updates | **148**

Junos OS Release Notes for PTX Series Packet Transport Routers

IN THIS SECTION

These release notes accompany Junos OS Release 20.1R1 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

Interfaces and Chassis

- **Handling thermal health events (PTX5000)**—Starting in Junos OS Release 20.1R1, on PTX5000 routers, you can enable a thermal health check and configure an action (such as auto shutdown and alarm) to be taken when a thermal health event such as power leakage is detected. You can also configure the power supply module (PSM) watchdog to shut down the PSM output power in case a thermal health event causes Junos to go down.

  > **NOTE:** The PSM watchdog feature works only if all the online PSMs in the router support this feature.

  [See Handling Thermal Health Events Using Thermal Health Check and PSM Watchdog]

- **Support for new show | display set CLI commands (ACX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the following new **show** commands have been introduced:

  - **show | display set explicit**—Display explicitly, as a series of commands, all the configurations that the system internally creates when you configure certain statements from the top level of the hierarchy.
  - **show | display set relative explicit**—Display explicitly, as a series of commands, all the configurations that the system internally creates when you configure certain statements from the current hierarchy level.

  [See show | display set and show | display set relative.]

Junos OS XML API and Scripting

- **The jcs:load-configuration template supports loading the rescue configuration (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the **jcs:load-configuration** template supports the **rescue** parameter to load and commit the rescue configuration on a device. SLAX and XSLT scripts can call the **jcs:load-configuration** template with the **rescue** parameter set to **"rescue"** to replace the active configuration with the rescue configuration.

  [See Changing the Configuration Using SLAX and XSLT Scripts and jcs:load-configuration Template.]

Junos Telemetry Interface

- **IS-IS adjacency and LSDB event streaming support on JTI (MX960, PTX1000, and PTX10000)**—Junos OS Release 20.1R1 provides IS-IS adjacency and link-state database (LSDB) statistics using Junos telemetry

interface (JTI) and remote procedure call (gRPC) services or gRPC Network Management Interface (gNMI) services. ON_CHANGE statistics are sent to an outside collector.

The following resource paths are supported:

- **/network-instances/network-instance/protocols/protocol/isis/interfaces/interfaces/circuit-counters/state/** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/interfaces/interface/levels/level/packet-counters/** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/system-level-counters/state/** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/interfaces/interfaces/levels/level/adjacencies/adjacency/state/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/extended-ipv4-reachability/prefixes/prefix/state/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/extended-ipv4-reachability/prefixes/prefix/subtlvs/subtlv/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv6-reachability/prefixes/prefix/state/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv6-reachability/prefixes/prefix/subtlvs/subtlv/** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/extended-is-reachability/neighbors/neighbors/subTLVs/subTLVs/adjacency-sid/sid/state/** (ON-CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/extended-is-reachability/neighbors/neighbors/subTLVs/subTLVs/lan-adjacency-sid/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv4-interfaces-addresses/state/** (ON_CHANGE))
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv4-srlg/state/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv4-te-router-id/state/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/ipv6-interfaces-addresses/state/** (ON_CHANGE)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/router-capabilities/router-capability/subtlvs/subtlv/segment-routing-capability/state/** (ON_CHANGE)

- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/state** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/area-address/state/address** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/nlpid/state/nlpid** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/lsp-buffer-size/state/size** (stream)
- **/network-instances/network-instance/protocols/protocol/isis/levels/level/link-state-database/lsp/tlvs/tlv/hostname/state/hname** (stream)

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

- **Platform, interface, and alarm sensor ON_CHANGE support on JTI (MX960, MX2020, PTX1000, PTX5000)**—Junos OS Release 20.1R1 supports platform, interface, and alarm statistics using Junos telemetry interface (JTI) and gRPC Network Management Interface (gNMI) services. You can use this feature to send ON_CHANGE statistics for a device to an outside collector.

  This feature supports the OpenConfig models:

  - **openconfig-platform.yang**: oc-ext:openconfig-version 0.12.1
  - **openconfig-interfaces.yang**: oc-ext:openconfig-version 2.4.1
  - **openconfig-alarms.yang**: oc-ext:openconfig-version 0.3.1

  Use the following resource paths in a gNMI subscription:

  - **/components/component** (for each installed FRU)
  - **/interfaces/interface/state/**
  - **/interfaces/interface/subinterfaces/subinterface/state/**
  - **/alarms/alarm/**

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

- **gRPC Dial-Out support on JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Junos OS Release 20.1R1 provides remote procedure call (gRPC) dial-out support for telemetry. In this method, the target device (server) initiates a gRPC session with the collector (client) and, when the session is established, streams the telemetry data that is specified by the sensor-group subscription to the collector. This is in contrast to the gRPC network management interface (gNMI) dial-in method, in which the collector initiates a connection to the target device.

  gRPC dial-out provides several benefits as compared to gRPC dial-in, including simplifying access to the target advice and reducing the exposure of target devices to threats outside of their topology.

To enable export of statistics, include the **export-profile** and **sensor** statements at the [**edit services analytics**] hierarchy level. The export profile must include the reporting rate, the transport service (for example, gRPC), and the format (for example, gbp-gnmi). The sensor configuration should include the name of the collector (the server's name), the name of the export profile, and the resource path. An example of a resource path is **/interfaces/interface[name='fxp0'**.

[See Using gRPC Dial-Out for Secure Telemetry Collection.]

- **gRPC version v1.18.0 with JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Junos OS Release 20.1R1 includes support for remote procedure call (gRPC) services version v1.18.0 with Junos telemetry interface (JTI). This version includes important enhancements for gRPC. In earlier releases, JTI is supported with gRPC version v1.3.0.

  Use gRPC in combination with JTI to stream statistics at configurable intervals from a device to an outside collector.

  [See gRPC Services for Junos Telemetry Interface.]

- **LLDP statistics, notifications, and configuration model for suppress-tlv-advertisement support on JTI (MX240, MX480, MX960, MX10003, PTX10008, PTX10016)**—Junos OS Release 20.1R1 provides remote procedure call (gRPC) streaming services support for attribute leaf **suppress-tlv-advertisement** under the resource path **/lldp/state/suppress-tlv-advertisement**. The following TLVs are supported, which in turn support operational state, notifications, and configuration change support:

  - port-description
  - system-name
  - system-description
  - system-capabilities
  - management-address
  - port-id-type

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

- **SR-TE statistics for uncolored SR-TE policies streaming on JTI (MX Series, PTX Series)**—Junos OS Release 20.1R1 provides segment routing traffic engineering (SR-TE) per label-switched Path (LSP) route statistics using Junos telemetry interface (JTI) and remote procedure call (gRPC) services. Using JTI and gRPC services, you can stream SR-TE telemetry statistics for uncolored SR-TE policies to an outside collector.

  Ingress statistics include statistics for all traffic steered by means of an SR-TE LSP. Transit statistics include statistics for traffic to the Binding-SID (BSID) of the SR-TE policy.

  To enable these statistics, include the **per-source per-segment-list** statement at the [**edit protocols source-packet-routing telemetry statistics**] hierarchy level.

  If you issue the **set protocols source-packet-routing telemetry statistics no-ingress** command, ingress sensors are not created.

If you issue the **set protocols source-packet-routing telemetry statistics no-transit** command, transit sensors are not created. Otherwise, if BSID is configured for a tunnel, transit statistics are created.

The following resource paths (sensors) are supported:

- **/junos/services/segment-routing/traffic-engineering/tunnel/lsp/ingress/usage/**
- **/junos/services/segment-routing/traffic-engineering/tunnel/lsp/transit/usage/**

To provision the sensor to export data through gRPC services, use the **telemetrySubscribe** RPC.

Streaming telemetry data through gRPC or gNMI also requires the OpenConfig for Junos OS module.

[See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface, source-packet-routing, and show spring-traffic-engineering lsp detail name *name*.]

Routing Protocols

- **Support for topology-independent loop-free alternate (TI-LFA) in IS-IS for IPv6-only networks (ACX Series, MX Series, and PTX Series)**— Starting with Junos OS Release 20.1R1, you can configure TI-LFA with segment routing in an IPv6-only network for the IS-IS protocol. TI-LFA provides MPLS fast reroute (FRR) backup paths corresponding to the post-convergence path for a given failure. TI-LFA provides protection against link failure, and node failure.

  You can enable TI-LFA for IS-IS by configuring the **use-post-convergence-lfa** statement at the **[edit protocols isis backup-spf-options]** hierarchy level. You can enable the creation of post-convergence backup paths for a given IPv6 interface by configuring the **post-convergence-lfa** statement at the **[edit protocols isis interface *interface-name* level *level*]** hierarchy level. The **post-convergence-lfa** statement enables link-protection mode.

  You can enable **node-protection** mode for a given interface at the **[edit protocols isis interface *interface-name* level *level* post-convergence-lfa]** hierarchy level. However, you cannot configure fate-sharing protection for IPv6-only networks.

  [See Understanding Topology-Independent Loop-Free Alternate with Segment Routing for IS-IS.]

MPLS

- **CoS-based forwarding and policy-based routing to steer selective traffic over an SR-TE path (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 20.1R1, you can use CoS-based forwarding (CBF) and policy-based routing (PBR, also known as filter-based forwarding or FBF) to steer service traffic using a particular segment routing-traffic-engineered (SR-TE) path. This feature is supported only on non-colored segment routing LSPs that have the next hop configured as a first hop label or an IP address.

  With CBF and PBR, you can:

  - Choose an SR-TE path on the basis of service.

- Choose the supporting services to resolve over the selected SR-TE path.

[See Example: Configuring CoS-Based Forwarding and Policy-Based Routing For SR-TE LSPs.]

- **Support for segment routing over RSVP forwarding adjacency (MX Series and PTX Series)**—Starting with Junos OS Release 20.1R1, we provide support for segment routing traffic to be carried over RSVP LSPs that are advertised as forwarding adjacencies in IS-IS. This feature is implemented in a network having LDP on the edge and RSVP in the core where you can easily replace LDP with IS-IS segment routing because it eliminates the need for MPLS signaling protocols such as LDP. This helps to remove a protocol from the network and results in network simplification.

  [See Understanding Segment Routing over RSVP Forwarding Adjacency in IS-IS.]

Network Management and Monitoring

- **Remote port mirroring to an IP address (GRE encapsulation) (PTX Series)**—You use port mirroring to send traffic to applications that analyze traffic to monitor compliance, enforce policies, detect intrusions, and so on. Starting in Junos OS Release 20.1R1, you can configure remote port mirroring to send sampled packets to a remote IP address, with the packets encapsulated in a GRE header.

  - Configure remote port mirroring to send sampled packets to a remote IP address, with the packets encapsulated in an IPv4 GRE header:

    set forwarding-options port-mirroring instance *instance-name* output ip-source-address *address* ip-destination-address *address*

  - (Optional) Configure a static traffic-class value that represents the 8-bit differentiated services (DS) field in the IPv4 header of a GRE tunnel. You can program 6 of the 8 bits, so the value that you can configure under DSCP can be 0-63 (2^0 to 2^6).

    set forwarding-options port-mirroring instance *instance-name* output dscp *numeric-dscp-value*

  - (Optional) Configure a policer to police the mirrored traffic that is going out of that interface:

    set forwarding-options port-mirroring instance *instance-name* output policer *policer-name*

  - (Optional) Configure the forwarding of packets to a queue defined by a forwarding class:

    set forwarding-options port-mirroring instance *instance-name* output forwarding-class *forwarding-class-name*

  [See instance (Port Mirroring) and traffic-class (Tunnels).]

- **On-box monitoring support on the control plane (MX Series and PTX Series)**—Starting in Junos OS Release 20.1R1, you can configure on-box monitoring to monitor anomalies with respect to the memory utilization of Junos OS applications and the overall system in the control plane of MX Series and PTX Series routers.

You can use on-box monitoring to monitor system-level memory and process-level memory to detect possible leaks. When the system is running low on memory, the process heuristic shares the prediction and you can configure the action to be taken when leaks are identified.

See memory (system)

System Management

- **Restrict option under NTP configuration is now visible (ACX Series, QFX Series, MX Series, PTX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the **noquery** command under the **restrict** hierarchy is now available and can be configured with a mask address. The **noquery** command is used to restrict ntpq and ntpdc queries coming from hosts and subnets.

  [See Configuring NTP Access Restrictions for a Specific Address.]

SEE ALSO

- What's Changed | **158**
- Known Limitations | **159**
- Open Issues | **160**
- Resolved Issues | **162**
- Documentation Updates | **166**
- Migration, Upgrade, and Downgrade Instructions | **166**

What's Changed

There are no changes in the behavior of Junos OS features or in the syntax of Junos OS statements and commands in this release for PTX Series.

SEE ALSO

- What's New | **151**
- Known Limitations | **159**
- Open Issues | **160**
- Resolved Issues | **162**
- Documentation Updates | **166**

Migration, Upgrade, and Downgrade Instructions | 166

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.

General Routing

- PTX Series platforms with the FPC-PTX-P1-A or FPC2-PTX-P1A line card might encounter a single event upset (SEU) event that can cause a linked-list corruption of the TQCHIP. The following syslog message is reported: **Jan 9 08:16:47.295 router fpc0 TQCHIP1: Fatal error pqt_min_free_cnt is zero Jan 9 08:16:47.295 router fpc0 CMSNG: Fatal ASIC error, chip TQ Jan 9 08:16:47.295 router fpc0 TQ Chip::FATAL ERROR!! from PQT free count is zero jan 9 08:16:47.380 router alarmd[2427]: Alarm set: FPC color=RED, class=CHASSIS, reason=FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 Jan 9 08:16:47.380 router craftd[2051]: Fatal alarm set, FPC 0 Fatal Errors - TQ Chip Error code: 0x50002** Junos OS chassis management error handling does detect such condition, and raises an alarm and performs the **disable-pfe** action for the affected Packet Forwarding Engine entity. To recover this Packet Forwarding Engine entity, a restart of the FPC is needed. Soft errors are transient or non-recurring. FPCs experiencing such SEU events do not have any permanent damage. Contact your Juniper support representative if the issue is seen after a FPC restart. PR1254415
- When a filter is attached in the outbound direction, GRE encapsulated headers are applied after the filter block in the egress direction. So in this case, it is possible that the filter is evaluated on an old header content (and not on the new GRE encapsulated header) and hence filter evaluation turns true and the new GRE encapsulated gets recirculated for another GRE encapsulation. This issue is difficult to fix as filter block evaluation happens before the new header is attached. PR1465837
- PTX1000/PTX10000 platform count MPLS header also in packet length where as MX does not include it when acting in egress PE role. So we see difference in byte accounting in both platforms corresponding to the length of MPLS label stack received with the packet. PR1482408

SEE ALSO

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

- PTX: CM2.0 : Alarm action is not working for minor error, after changing the threshold to 1. PR1345154
- Traffic loss is greater than 50 ms (in order of 200 to 300 ms) for IP routes pointing to unilist of composites with indirect next hops during a link down scenario. In this case, the Packet Forwarding Engine does not do the local repair and will wait for the rpd to install the new next hops. PR1383965
- On routers and switches running Junos OS, with Link Aggregation Control Protocol (LACP) enabled, deactivating a remote aggregate Ethernet (AE) member link makes the local member link move to LACP Detached state. The detached link is invalidated from the Packet Forwarding Engine AE-Forwarding table as expected. However, if the device is rebooted with this state, all the member links are enabled in the Packet Forwarding Engine AE-Forwarding table irrespective of LACP states, which results in traffic drop. PR1423707

- The em2 interface configuration is causing the FPC to crash during initialization, and the FPC does not come online, after deleting the em2 configuration and restarting the router, FPC comes online. PR1429212
- Memory leaks are expected in this release. PR1438358
- On PTX1000 and PTX10002 platforms, if transient voltage fluctuations on a SIB or an FPC are seen, it might trigger the fabric healing process (FHP) and FPC/SIB restart. Later, the SIB might not restart but the FPC still goes online, so the device might experience silent dropping of packets, which affects the service. PR1460406
- When users configure the best destination network with **dyn-tunnel-attribute-policy** and preference, we are not migrating, the tunnel from the old destination network. PR1462805
- Using a PTX system with an FPC2-PTX-P1A or an FPC-PTX-P in a network with a high rate of multicast routes changes -- that is, active PIM, or MVPN environment-- might lead to PLCT **Policer and Counter** counter exhaustion. When PLCT counter entries are exhausted, PTX router may start to lose protocols' adjacencies to its neighbors, or transit/ingress LSPs may go down. PR1479789
- On a PTX3000 or PTX5000 platform with some specific FPCs, if the weights of links are set to an invalid value on an AE bundle interface or unilist (an unilist next hop composed of several unicast next-hops), an FPC crash might be observed. It is a rare issue and the FPC will try to reload to resolve this problem. Traffic loss might be seen before the FPC completes the reload period. PR1484255
- On all Junos based PTX/QFX10000 Series platforms with large filter configuration (for example, one filter has more than 500 terms or one term has more than 500 filters) scenario, during the change operation of loopback0 filter, the bfd sessions start to flap. PR1491575
- During FRR event, if the backup path is inet table lookup(with backup-ip-forward configuration) then, per Sid-stats might not work as expected on PTX Series platform only. This problem is not seen on MX routers. Traffic loss during FRR switchover is more than 50 ms on some occasions. PR1491765

Infrastructure

- The harmless log of **invalid SMART checksum** might be seen when performing software upgrade to specific releases (for example, Junos OS Releases 15.1F5-S3, 15.1F6-S1, 15.1F7, 15.1R4-S3, 15.1R5, 16.1R1, 16.1R2, and 16.2R1). PR1222105

MPLS

- When the two directly connected BGP peers are established over MPLS LSP, if the IP layer's MTU is smaller than the MPLS layer's MTU, and also the BGP packets from the host have the DF bit set, the BGP session might keep flapping because of the incorrect TCP-MSS in use. PR1493431

Routing Protocols

- With Bidirectional Forwarding Detection (BFD) configured on an aggregated Ethernet interface, if you disable and then enable the aggregated Ethernet interface, then that interface and the BFD session might not come up. PR1354409
- By adding the sbfd responder configuration on RE-DUO-2600, ppmd crashes and a core file is generated. The issue is not seen on RE-PTX-2X00x6(NGRE). PR1477525

SEE ALSO

What's New | **151**

What's Changed | **158**

Known Limitations | **159**

Resolved Issues | **162**

Documentation Updates | **166**

Migration, Upgrade, and Downgrade Instructions | **166**

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in this release for PTX Series.

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

Forwarding and Sampling

- The pfed might crash and be unable to come up on the PTX Series or TVP platforms. PR1452363

General Routing

- PTX Series interface stays down after maintenance. PR1412126
- Telemetry statistics might not account correctly when IS-IS sensors are enabled and the route next hops are ae interfaces. PR1413680
- LACP packet does not pass through Layer 2 circuit. PR1424553
- Interface does not come up after interface flapping and FPC reboot. PR1428307
- Reclassification policy applied on the route prefixes might not work on PTX Series platforms. PR1430028
- The l2cpd process might crash and generate a core file when interfaces are flapping. PR1431355
- The FPC might crash when a firewall filter is modified. PR1432116
- Unable to change DDoS protocol TTL values under PTX10000. PR1433259
- Upgrading fails due to communication failure between Junos VM and the host OS. PR1438219
- Packet loss might be seen if IPoIP or MPLS-over-UDP dynamic tunnels with ECMP are configured. PR1446132
- Changing the hostname triggers an on-change notification, not an adjacency on-change notification. Also, currently IS-IS is sending the hostname instead of the system ID in OC paths. PR1449837
- JNP10K-LC2101 FPC generates the "Voltage Tolerance Exceeded" major alarm for EACHIP 2V5 sensors. PR1451011

- The 100-Gbps interface might not come up after flapping on PTX5000. PR1453217
- Traffic might be dropped on PTX Series platforms. PR1459484
- Silent dropping of traffic upon interface flapping after DRD auto-recovery. PR1459698
- The "forwarding" option is missed in routing-instance type. PR1460181
- Hardware failure in CB2-PTX causes traffic interruption. PR1460992
- The **sample**, **syslog**, or **log** action in output firewall filters for packets of size less than 128 bytes might cause an ASIC wedge (all packet loss) on PTX Series platforms. PR1462634
- PIC might restart if the temperature of QSFP optics is overheated on PTX3000 or PTX5000. PR1462987
- An FPC might restart during runtime on PTX10000 or QFX10000 lines of devices. PR1464119
- Continuous MACsec-wedge-cleared logs might be seen and LACP flapping might happen with 100% line-rate traffic or near line rate traffic in the MACsec line card. PR1466481
- EBUF parity interrupt is not seen on PTX Series routers or the QFX10000 line of switches. PR1466532
- IPv6 traffic might get dropped in a Layer 3 VPN network. PR1466659
- Packet Forwarding Engine error logs (prds_packet_classify_notification: Failed to find fwd nh for flabel 48) might be reported when IGMP packets get sampled on the PTX5000 platform. PR1466995
- Optics measurements might not be streamed for interfaces of a PIC over JTI. PR1468435
- Incorrect counter value for **Arrival rate** and **Peak rate** for DDoS commands. PR1470385
- Traffic loops for pure Layer 2 packets coming over an EVPN tunnel with the destination MAC address matching the IRB MAC address. PR1470990
- The **input-vlan-map** or **output-vlan-map** might not work properly in a Layer 2 circuit local-switching scenario. PR1474876

Infrastructure

- The kernel crashes when removing a mounted USB storage device while a file is being copied to it. PR1425608
- Slow response from SNMP might be observed after an upgrade to Junos OS Release 19.2R1 and later. PR1462986

Interfaces and Chassis

- After member interface flapping, the aggregated Ethernet remains down on the 5-port 100-Gigabit Ethernet DWDM CFP2-ACO PIC. PR1429279

Layer 2 Ethernet Services

- Member links state might be asychronized on a connection between the PE and CE devices in EVPN A/A scenario. PR1463791

MPLS

- Kernel crash and device restart might happen. PR1478806

Routing Protocols

- SSH login might fail if a user account exists in both local database and RADIUS or TACACS+. PR1454177
- The **other querier present interval** timer cannot be changed in an IGMP/MLD snooping scenario. PR1461590
- The rpd process might crash with BGP multipath and route withdrawal occasionally. PR1481589

SEE ALSO

What's New | **151**

What's Changed | **158**

Known Limitations | **159**

Open Issues | **160**

Documentation Updates | **166**

Migration, Upgrade, and Downgrade Instructions | **166**

Documentation Updates

IN THIS SECTION

This section lists the errata and changes in Junos OS Release 20.1R1 documentation for the PTX Series.

Dynamic Host Configuration Protocol (DHCP)

- **Introducing DHCP User Guide**—Starting in Junos OS Release 20.1R1, we are introducing the DHCP User Guide for Junos OS routing, switching, and security platforms. This guide provides basic configuration details for your Junos OS device as DHCP Server, DHCP client, and DHCP relay agent.

  [See DHCP User Guide.]

SEE ALSO

- What's New | 151
- What's Changed | 158
- Known Limitations | 159
- Open Issues | 160
- Resolved Issues | 162
- Migration, Upgrade, and Downgrade Instructions | 166

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.

Basic Procedure for Upgrading to Release 20.1

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

> **NOTE:** Back up the file system and the currently active Junos OS configuration before upgrading Junos OS. This allows you to recover to a known, stable environment if the upgrade is unsuccessful. Issue the following command:
>
> ```
> user@host>request system snapshot
> ```

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

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

To download and install Junos OS Release 20.1R1:

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

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

2. Select the name of the Junos OS platform for the software that you want to download.

3. Select the release number (the number of the software version that you want to download) from the Release drop-down list to the right of the Download Software page.

4. Select the **Software** tab.

5. In the Install Package section of the Software tab, select the software package for the release.

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

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

10. Install the new **jinstall** package on the router.

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

All customers except the customers in the Eurasian Customs Union (currently 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-x86-64-20.1R1.9.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-x86-64-20.1R1.9-limited.tgz
```

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

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

- **scp://*hostname*/*pathname***

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: You need to install the Junos OS software package and host software package on the routers with the RE-PTX-X8 Routing Engine. For upgrading the host OS on this router with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the **request vmhost software add** command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.

NOTE: After you install a Junos OS Release 20.1**jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.4, 18.1, and 18.2 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from

Junos OS Release 17.1 to Release 17.3. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

Upgrading a Router with Redundant Routing Engines

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

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

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

SEE ALSO

What's New | **151**

What's Changed | **158**

Known Limitations | **159**

Open Issues | **160**

Resolved Issues | **162**

Documentation Updates | **166**

Junos OS Release Notes for the QFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 20.1R1 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

NOTE: The following QFX Series platforms are supported in Release 20.1R1: QFX5100, QFX5110 (32Q and 48S), QFX5120, QFX5200, QFX5200-32CD, QFX5210, QFX10002, QFX10002-60C, QFX10008, and QFX10016.

Junos on White Box runs on Accton Edgecore AS7816-64X switches in this release. The software is based on Junos OS running on QFX5210 switches, so release-note items that apply to QFX5210 switches also apply to Junos on White Box.

EVPN

- **Routing traffic between a VXLAN and a Layer 3 logical interface (EX4650 and QFX5120)—**Starting in Junos OS Release 20.1R1, EX4650 and QFX5120 switches support the routing of traffic between a Virtual Extensible LAN (VXLAN) and a Layer 3 logical interface. This feature is enabled by default, so you do not need to take any action to enable it.

  > **NOTE:** By default, this feature is disabled on QFX5110 switches. To enable the feature on QFX5110 switches, you must perform the configuration described in Understanding How to Configure VXLANs and Layer 3 Logical Interfaces to Interoperate.

  (You can configure the Layer 3 logical interface using the **set interfaces *interface-name* unit *logical-unit-number* family inet address *ip-address/prefix-length*** or the **set interfaces *interface-name* unit *logical-unit-number* family inet6 address *ipv6-address/prefix-length*** command.)

High Availability (HA) and Resiliency

- **Inline keepalive packet support for BFD (QFX5110, QFX5120, QFX5200, and QFX5210)**—Starting in Junos OS Release 20.1R1, multihop BFD inline keepalive support enables scaling up to 10 inline BFD sessions with 150-millisecond support on both multihop BFD sessions as well as single-hop inline sessions. Multihop BFD session intervals can also be configured to less than 1-second granularity. This enables both faster detection of link failures and recovery. The switch will also send keepalive messages according to the configured interval.

  > **NOTE:** This feature only applies for IPv4 multihop BFD sessions and standalone BFD sessions. This feature is not supported for micro BFD implementation.

  [See Understanding Bidirectional Forwarding Detection (BFD).]

Interfaces and Chassis

- **Support for static link protection on aggregated interfaces (EX4650, QFX5120-32C, and QFX5120-48Y)**—Starting in Junos OS Release 20.1R1, you can enable link protection on aggregated interfaces for a specified static label-switched path (LSP). You can designate a primary and a backup physical link to support link protection. Egress traffic passes only through the designated primary link. This traffic includes transit traffic and locally generated traffic on the router. When the primary link fails, traffic is routed through the backup link.

  [See link-protection.]

- **Support for new show | display set CLI commands (ACX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the following new **show** commands have been introduced:
  - **show | display set explicit**—Display explicitly, as a series of commands, all the configurations that the system internally creates when you configure certain statements from the top level of the hierarchy.
  - **show | display set relative explicit**—Display explicitly, as a series of commands, all the configurations that the system internally creates when you configure certain statements from the current hierarchy level.

  [See show | display set and show | display set relative.]

Junos OS XML, API, and Scripting

- **The jcs:load-configuration template supports loading the rescue configuration (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the **jcs:load-configuration** template supports the **rescue** parameter to load and commit the rescue configuration on a device. SLAX and XSLT scripts can call the **jcs:load-configuration** template with the **rescue** parameter set to **"rescue"** to replace the active configuration with the rescue configuration.

  [See Changing the Configuration Using SLAX and XSLT Scripts and jcs:load-configuration Template.]

Junos Telemetry Interface

- **gRPC Dial-Out support on JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Junos OS Release 20.1R1 provides remote procedure call (gRPC) dial-out support for telemetry. In this method, the target device (server) initiates a gRPC session with the collector (client) and, when the session is established, streams the telemetry data that is specified by the sensor-group subscription to the collector. This is in contrast to the gRPC network management interface (gNMI) dial-in method, in which the collector initiates a connection to the target device.

  gRPC dial-out provides several benefits as compared to gRPC dial-in, including simplifying access to the target advice and reducing the exposure of target devices to threats outside of their topology.

  To enable export of statistics, include the **export-profile** and **sensor** statements at the [**edit services analytics**] hierarchy level. The export profile must include the reporting rate, the transport service (for example, gRPC), and the format (for example, gbp-gnmi). The sensor configuration should include the name of the collector (the server's name), the name of the export profile, and the resource path. An example of a resource path is **/interfaces/interface[name='fxp0'**.

  [See Using gRPC Dial-Out for Secure Telemetry Collection.]

- **gRPC version v1.18.0 with JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Junos OS Release 20.1R1 includes support for remote procedure call (gRPC) services version v1.18.0 with Junos telemetry

interface (JTI). This version includes important enhancements for gRPC. In earlier releases, JTI is supported with gRPC version v1.3.0.

Use gRPC in combination with JTI to stream statistics at configurable intervals from a device to an outside collector.

[See gRPC Services for Junos Telemetry Interface.]

Multicast

- **PIM with IPv6 multicast traffic (EX4650 and QFX5120-48Y)**—Starting in Junos OS Release 20.1R1, EX4650 and QFX5120-48Y switches support Protocol Independent Multicast (PIM) with IPv6 multicast traffic as follows:
  - PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode (PIM-SDM)
  - PIM any-source multicast (PIM-ASM) and PIM source-specific multicast (PIM-SSM)
  - Static, embedded, and anycast rendezvous points (RPs)

[See PIM Overview.]

Routing Policy and Firewall Filters

- **Support for flexible-match-mask match condition (EX4650 and QFX-Series)**—Starting with Junos OS Release 20.1R1, for EX4650, QFX5120-32C, and QFX5120-48Y switches, the **flexible-match-mask** match condition in firewall filters is supported for the **inet**, **inet6**, and **ethernet-switching** families. With this feature, you can configure a filter by specifying the length of the match (4 bytes maximum) starting from a Layer 2 or Layer 3 packet offset.

  [See Firewall Filter Flexible Match Conditions.]

Routing Protocols

- **Redistribution of IPv4 routes with IPv6 next hop into BGP (QFX Series)**—Starting in Release 20.1R1, devices running Junos OS can forward IPv4 traffic over an IPv6-only network, which generally cannot forward IPv4 traffic. As described in RFC 5549, IPv4 traffic is tunneled from CPE devices to IPv4-over-IPv6 gateways. These gateways are announced to CPE devices through anycast addresses. The gateway devices then create dynamic IPv4-over-IPv6 tunnels to remote CPE devices and advertise IPv4 aggregate routes to steer traffic. Route reflectors with programmable interfaces inject the tunnel information into the network. The route reflectors are connected through IBGP to gateway routers, which advertise the IPv4 addresses of host routes with IPv6 addresses as the next hop.

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

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

Software Defined Networking

- **VMware NSX Data Center for vSphere 6.4.5 and 6.4.6 certification (QFX5100 Virtual Chassis)**—Starting with Junos OS Release 20.1R1, Juniper Networks certifies QFX5100 Virtual Chassis as a hardware Virtual Extensible LAN (VXLAN) gateway in an Open vSwitch Database (OVSDB) and VXLAN network with a VMware NSX Data Center for vSphere 6.4.5 or 6.4.6 controller.

  [See OVSDB-VXLAN User Guide for QFX Series Switches (VMware NSX).]

Storage and Fibre Channel

- **FIP snooping (EX4650-48Y and QFX5120-48Y)**—Starting in Junos OS Release 20.1R1, EX4650-48Y and QFX5120-48Y switches support Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) snooping. With FIP snooping enabled on these switches, you prevent unauthorized access and data transmission to a Fibre Channel (FC) network by permitting only those servers that have logged in to the FC network to access the network. You enable FIP snooping on FCoE VLANs when the switch is being used as an FCoE transit switch that connects FC initiators (servers) on the Ethernet network to FCoE forwarders at the FC storage area network (SAN) edge.

  [See Understanding FCoE Transit Switch Functionality and Understanding VN_Port to VN_Port FIP Snooping on an FCoE Transit Switch.]

System Management

- **Support for the Precision Time Protocol (PTP) AES67, SMPTE ST-2059-2, and AES67+SMPTE profiles (QFX10002)**—Starting in Junos OS Release 20.1R1, you can enable the AES67, SMPTE ST-2059-2, and AES67+SMPTE profiles to support video applications for capture (for example, cameras), video edit, and playback to be used in professional broadcast environments. The PTP standard allows multiple video sources to stay in synchronization across various equipment by providing time and frequency synchronization to all devices. These profile support PTP over IPv4 multicast and ordinary and boundary clocks.

  To configure the AES67, SMPTE ST-2059-2, and AES67+SMPTE profiles, enable one of the **aes67**, **smpte**, or **aes67-smpte** statements at the **[edit protocols ptp profile-type]** hierarchy level.

  [See Understanding the PTP Media Profiles.]

- **Restrict option under NTP configuration is now visible (ACX Series, QFX Series, MX Series, PTX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the **noquery** command under the **restrict** hierarchy is now available and can be configured with a mask address. The **noquery** command is used to restrict ntpq and ntpdc queries coming from hosts and subnets.

  [See Configuring NTP Access Restrictions for a Specific Address.]

SEE ALSO

What's Changed | **178**

Known Limitations | **180**

Open Issues | **181**

Resolved Issues | **186**

Documentation Updates | **193**

Migration, Upgrade, and Downgrade Instructions | **194**

What's Changed

IN THIS SECTION

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

Class of Service (CoS)

- We've corrected the output of the **show class-of-service interface | display xml** command. The output is of the following sort: <container> <leaf-1> data </leaf-1><leaf-2>data </leaf-2> <leaf-3> data</leaf-3> <leaf-1> data </leaf-1> <leaf-2> data </leaf-2> <leaf-3> data </leaf-3> </container> will now appear correctly as <container> <leaf-1> data </leaf-1><leaf-2>data </leaf-2> <leaf-3> data</leaf-3></container> <container> <leaf-1> data </leaf-1> <leaf-2> data </leaf-2> <leaf-3> data </leaf-3> </container>.

Interfaces and Chassis

- **Commit error thrown when GRE interface and tunnel source interface are configured in different routing instances (QFX Series)**—In Junos OS Release 20.1R1, QFX Series switches do not support configuring the GRE interface and the underlying tunnel source interface in two different routing instances. If you try this configuration, it will result in a commit error with the following error message:

  error: GRE interface (gr-0/0/0.0) and its underlying tunnel source interface are in different routing-instances

  error: configuration check-out failed

  [See Understanding Generic Routing Encapsulation.]

- **Support for 100-Mbps speed using QFX-SFP-1GE-T on QFX5110-48S Switches**—Starting in Junos OS release 20.1R1, in addition to 1-Gbps, 10-Gbps, 40-Gbps, 100-Gbps speeds, now you can configure 100-Mbps speed using the **set interfaces *interface-name* speed 100M** command. By default, all 48 ports on QFX5110-48S come up with 10-Gbps speed. With QFX-SFP-1GE-T connected, along with 1-Gbps speed, now you can also configure 100-Mpbs on QFX5110-48S switches.

[See Speed (Ethernet)].

- **Logical Interface is created along with physical Interface by default (EX Series switches, QFX Series switches, MX Series routers)**—The logical interface is created on ge, et, xe interfaces along with the physical interface, by default. In earlier Junos OS Releases, by default, only physical interfaces were created. For example, for ge interfaces, earlier when you view the **show interfaces** command, by default, only the physical interface (ge-0/0/0), was displayed. Now, the logical interface (ge-0/0/0.16386) is also displayed.

Multicast

- **Multicast Layer 2 transit traffic statistics by multicast source and group (EX4600, EX4650, and the QFX5000 line of switches)**—Starting in Junos OS Release 20.1R1, EX4600, EX4650, and the QFX5000 line of switches provide statistics on the packet count for each multicast group and source when passing multicast transit traffic at Layer 2 with IGMP snooping. Run the **show multicast snooping route extensive** CLI command to see this count in the **Statistics: ... *n* packets** output field. The other statistics in that output field, **kBps** and **pps**, are not available (values displayed there are not valid statistics for multicast traffic at Layer 2). In earlier Junos OS releases, all three values in the **Statistics** output field for **kBps**, **pps**, and **packets** do not provide valid statistics for multicast traffic at Layer 2.

  [See show multicast snooping route.]

Network Management and Monitoring

- **entPhysicalTable fetched on QFX10002**—In Junos OS Release 20.1R1, the MIB data for entPhysicalTable will be fetched on a QFX10002-72Q or QFX10002-36Q switch.

  [See SNMP Explorer.]

Routing Protocols

- **Automatic installation of YANG-based CLI for RIFT protocol (MX Series, QFX Series, and vMX with 64-bit and x86-based servers)**—In Rift 1.2 Release, installation of the CLI for RIFT protocol occurs automatically along with the installation of the junos-rift package. In the pre-1.0 releases of the junos-rift package, the RIFT CLI had to be installed separately using **request system yang** command after installation of the junos-rift package.–

SEE ALSO

What's New | 171

Known Limitations | 180

Known Limitations

IN THIS SECTION

Learn about known limitations in Junos OS Release 20.1R1 for QFX Series. For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Class of Service (CoS)

- On QFX5100 platforms, due to major third-party SDK upgrade in 20.1R1 (from SDK 6.3.7 to 6.5.16), ISSU is not supported from any earlier releases to Junos OS Release 20.1R1. PR1479439

General Routing

- Downgrade from a TVP image to a non-TVP image is not supported. However, upgrade from a non-TVP image to a TVP image is supported. PR1345848
- During software validation, Junos OS mounts the new image and validates the configuration against the new image. Since the TVP-based QFX Series platforms (QFX5000 and QFX10000) are already mounting the maximum 4 disks during normal execution, it cannot mount the extra disk for this purpose. Thus QFX currently does not support configuration validation during upgrade on QFX5000 so the syntax error appears when the image installation is triggered with "validation". PR1421378

Infrastructure

- If Junos OS panics with a file-system-related panic, such as **dup alloc**, recovery through the OAM shell might be needed. From the OAM shell, run **fsck** on the root volume until it is marked clean. Only at this point, it is safe to reboot to the normal volume. PR1444941

Layer 2 Ethernet Services

- In an EVPN multihomed active/active scenario, when LACP is enabled on PE-CE child member links, the LACP force-up feature should not be enabled in conjunction with EVPN core isolation feature (enabled by default) because it is currently not supported in this scenario as these two features are contradictory in terms of the action they take. PR1461581

SEE ALSO

What's New | **171**

What's Changed | **178**

Open Issues | **181**

Resolved Issues | **186**

Documentation Updates | **193**

Migration, Upgrade, and Downgrade Instructions | **194**

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 20.1R1 for QFX Series. For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Class of Service (CoS)

- When CPU Q cells (memory) are exhausted, even though the incoming packet rate is less than the allowed bandwidth, you observe DDoS violations. PR1381775
- The priority-based flow control (PFC) feature is not supported on QFX5120 2-member Virtual Chassis currently due to hardware limitation. PR1431895

EVPN

- In EVPN-VXLAN core isolation scenario, the server is multihomed to the leaf devices through LACP interfaces. If graceful restart is enabled, upon system reboot or restart routing on the leaf device, the core isolation does not work. In the system reboot case, the issue results in the leaf device silently dropping the traffic sent from the server during the time window between LACP coming up and BGP coming up. In the restart routing case, there might be no traffic drop because of the graceful restart. PR1461795
- Bum traffic loop happen when core interface is isolated in short time period. Loop prevention feature does not work because CE interface is not flapped with core interface isolation. Routing Engine sets CE interface down after BGP hold time expired and Routing Engine sets CE interface to up after BGP session established. Default BGP hold time is 90 seconds. It needs 90 seconds to flap CE interface. Bum traffic can be looped till local bias filter is restored. PR1492784

General Routing

- Intermittent traffic loss is observed with RTG streams while flapping the RTG primary interface. PR1388082
- On QFX5110 and QFX5120 platforms, unicast RPF check in strict mode might not work properly. PR1417546
- On QFX Series Virtual Chassis during shutdown, if an interrupt is received, host incorrectly think that VM is hung triggering hardware watchdog NMI and generates a core file. PR1421250
- On switches running Junos OS with LACP enabled, deactivating a remote aggregate Ethernet member link makes the local member link move to LACP detached state. The detached link is then invalidated from the Packet Forwarding Engine aggregated Ethernet-Forwarding table as expected. However, if the device is rebooted with this state, all the member links are enabled in the Packet Forwarding Engine aggregated Ethernet-Forwarding table irrespective of LACP states, which results in traffic drop. PR1423707

- When you restart the routing process, if the system is configured with EVPN service, memory of the Layer 2 learning daemon increases by 4000 when you use **show system processes extensive | match l2ald**. PR1435561
- The unified ISSU is not supported on QFX5200 switches and fails from Junos OS Release 17.2X75-D4(x) to Junos OS Release 19.2R1. Also, dcpfe crash might be seen. PR1438690
- The time taken to install or delete IPv4 or IPv6 routes into the FIB is slowed down in Junos OS Release 19.3. Analysis shows that rpd learning rates are not degraded but RIB-to-FIB download rate is degraded. PR1441737
- On QFX10000 platforms, in an EVPN-VXLAN (spine-leaf) scenario, the QFX10000 spine switches are configured with VXLAN Layer 3 gateway (utilizing the virtual gateway) on an IRB interface. If you enable and then subsequently remove the VXLAN Layer 3 gateway on this IRB interface on one or some of these spine switches, traffic drop might be observed. As a workaround, configure all virtual gateways with unique IPv4 or IPv6 MAC address. PR1446291
- Whenever any member in a Remote Switched Port Analyzer (RSPAN) VLAN is removed from that VLAN, you must reconfigure the analyzer session for that RSPAN VLAN. PR1452459
- In EVPN-VXLAN with service provider style configuration, if the VLAN name associated with access ports is changed, then the virtual bridge domain might not be created. This is because the bridge domain add notification for the new VLAN comes before the bridge domain delete notification for the old VLAN. Because of this, the virtual bridge domain might not be created and MAC learning does not happen. PR1454095
- On QFX5110 with QSFP-100GBASE-SR4 optics made by Avago cannot link up. Use the **show chassis pic pic-slot 0 fpc-slot 0** command to identify the manufacturer of the optics. PR1457266
- In overall commit time, mostly mustd constraints evaluation takes 2 seconds extra because of the **persist-group-inheritance** feature made as default in the latest releases. However, this feature helps in improving the next subsequent commit times significantly in case of scaled configuration. The **persist-groups-inheritance** feature would be useful in customer scenarios where groups and nested groups are used extensively. In those scenarios, the groups inheritance path will not be built every time hence subsequent commits would be faster. PR1457939
- The output of the **show chassis environment** command can be seen from backup members as well. The issue is common to all QFX Series platforms. PR1474520
- Interfaces are not detected on some of the ports when we swap the 25-gigabit SFP transceiver and insert a 10-gigabit transceiver. PR1475574
- On QFX5220 platforms, when a lo0 firewall filter (inet/inet6) is used, Layer 3 forwarding traffic might be discarded by the lo0 filter. PR1475620
- PTP lock state stays in phase aligned after you disable ptp0 interface configured as slave interface with media profile. Instead of disabling ptp0 port, you can delete ptp0 interface to achieve the same result. PR1487505

- On QFX5100 switches, if more than one UDF filter or term is configured, then only the first filter or term will be programmed in the hardware because of SDK 6.5.16 upgrade. PR1487679
- On QFX10002 switches with **mclag** configurations, traffic drops when you deactivate or activate **ifd** trigger. PR1488166
- On QFX10000 Series platforms with large filter configuration (for example, one filter has more than 500 terms or one term has more than 500 filters) scenario, during the change operation of **loopback0** filter, the BFD sessions start to flap. PR1491575
- On QFX5100 switches, NSSU from earlier release to 20.1R1 might not work. As a workaround, normal upgrade from earlier release to 20.1R1 can be done. PR1496765

Interfaces and Chassis

- Multicast traffic can be flooded for 15 to 20 seconds to both MC-LAG peers, after the following sequence of steps:

  1. Disable or enable ICL.
  2. Reboot one of MC-LAG peers.
  3. Disable or enable a member link of ICL.

  This results in no traffic loss, and one of the MC-LAG nodes processes duplicate packets during this time period. PR1422473
- Flooding of ARP reply unicast packets is seen as a result of an ARP request sent for the device's VRRP MAC address. The ARP reply, which is flooded in the VLAN by the device, has the correct DMAC of the originator of the ARP request. In other words, the ARP reply is flooded but with the correct unicast DMAC. The ARP reply is not broadcasted.PR1454764

Layer 2 Features

- On QFX5110 and QFX5200 platforms, if storm control is enabled on the interfaces along VXLAN configuration, storm control will not take effect with the number of incoming ARP REQ packets than storm control threshold. PR1469837
- On QFX5000 platforms, you might see the **pools exhausted for Table:EGR_DVP_ATTRIBUTE** error message when statistics requests exceeded the supported scale because of the limited pool resources used for statistics collection on the hardware. There is no functional impact except for statistics collection for some hardware counters for which flex counter allocation failed for the time, the limit is exceeded. The statistics counters start functioning normally without manual change when the pool comes back to normal limit. PR1479826
- On QFX5100 switches, FXPC CPU utilization is increased due to high number of active ports after third-party SDK upgrade to 6.5.x from 5.3.x. PR1480132

Layer 2 Ethernet Services

- The DHCP DECLINE packets are not forwarded to the DHCP server when **forward-only** is set within **dhcp-reply**. PR1429456

Multiprotocol Label Switching (MPLS)

- In case the two directly connected BGP peers are established over MPLS LSP, if the IP layer's MTU is smaller than the MPLS layer's MTU and the BGP packets from the host have the DF bit set, the BGP session might keep flapping because of the wrong TCP MSS in use. PR1493431

Routing Protocols

- DCPFE core file is generated after watchdog trigger caused by the failed MAC deletion notification. The following repeated messages before the core file generation can be an evidence of the problem: **BRCM_SALM:brcm_salm_periodic_clear_pending(),125: Failed to delete Pendingentres for unit = 0, tgid = 1, err code = -9**. PR1371092
- On QFX5100 Virtual Chassis or Virtual Chassis Fabric, when the mini-PDT-base configuration is issued, the following error message is seen in the hardware: **BRCM_NH-,brcm_nh_bdvlan_ucast_uninstall(), 128:l3 nh 6594 unintsall failed**. There is no functionality impact because of this error message. PR1407175
- BGP route addition and deletion time and BGP, OSPF, and IS-IS link flap convergence time are increased in Junos OS Release 19.4. PR1464572
- MUX state of LACP interface does not change sometimes when **force-up** is configured. PR1484523

SEE ALSO

What's New | **171**

What's Changed | **178**

Known Limitations | **180**

Resolved Issues | **186**

Documentation Updates | **193**

Migration, Upgrade, and Downgrade Instructions | **194**

Resolved Issues

IN THIS SECTION

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

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

Class of Service (CoS)

- Shaping does not work after the reboot if **shaping-rate** is configured. PR1432078
- The traffic is placed in the network-control queue on an extended port even if it comes in with a different DSCP marking. PR1433252
- On QFX5120 switches, when you move unicast traffic to a multicast queue through an MF classifer, the **show interface queue** command does not display any status. PR1459281

EVPN

- The rpd might crash with EVPN-related configuration changes in a static VXLAN to MPLS stitching scenario. PR1467309

Forwarding and Sampling

- Type 1 ESI/AD route might not be generated locally on an EVPN PE device in the **all-active** mode. PR1464778

General Routing

- On QFX5100 Virtual Chassis, **MacDrainTimeOut and bcm_port_update failed: Internal error** is observed. PR1284590
- The **show chassis errors active detail** command is not supported on QFX5000 platforms. PR1386255
- The 10-Gigabit Ethernet fiber interfaces might flap frequently when they are connected to other vendor's switch. PR1409448
- The optic comes with Tx enabled by default. As the port is administratively disabled, the port is stopped but as the port has not been started, it does not disable Tx. PR1411015
- Part of routes could not be provided into the Packet Forwarding Engine when both IPv4 and IPv6 are used. PR1412873
- The **show interface** command shows **Media type: Fiber** on QFX5100-48T switches running "QFX 5e Series" image. PR1419732
- Ports might get incorrectly channelized if they are channelized to 10-Gbps and they are again channelized to 10-Gbps. PR1423496
- CoS rewrite rules applied under an aggregated Ethernet interface might not take effect after nonstop software upgrade (NSSU). PR1430173
- The l2cpd process might crash and generate a core file when interfaces flap. PR1431355
- The FPC might crash when a firewall filter is modified. PR1432116
- When you plug in an unsupported SFP-T module, the line card might crash. PR1432809
- BGP neighborship might not come up if the MACsec feature is configured. PR1438143
- QFX5100 Virtual Chassis does not come up after you replace a Virtual Chassis port fiber connection with a DAC cable. PR1440062
- MAC addresses learned on RTG might not be aged out after a Virtual Chassis member is rebooted. PR1440574

- Packet loss might be seen if IPoIP or MPLS-over-UDP dynamic tunnels are configured with ECMP. PR1446132
- On QFX5100 Virtual Chassis, a cyclic redundancy check (CRC) error might be seen on the Virtual Chassis Port (VCP). PR1449406
- Except one aggregated Ethernet member link, the other links do not send out sFlow sample packets for ingress traffic. PR1449568
- The em0 route might be rejected after the em0 interface is disabled and then enabled. PR1449897
- FPC does not restart immediately after rebooting the system. This might cause packet loss. PR1449977
- On QFX10000 platforms, CoS classification does not work. PR1450265
- The l2ald and eventd process are hogging 100 percent after the **clear ethernet-switching table** command is issued. PR1452738
- The classifier configuration does not get applied to the interface in an EVPN-VXLAN environment. PR1453512
- The **show chassis led** command shows incorrect status. PR1453821
- On QFX5100 Virtual chassis, VGD process hogs the CPU without the **switch-options vtep-source-interface lo0.0** configuration. PR1454014
- On QFX5110 Virtual Chassis, master FPC might come up in master state again after reboot instead of backup. PR1454343
- On QFX5000 platform, the dcpfe process crashes because usage of data which is not NULL is terminated. PR1454527
- On QFX10002-60C EVPN-VXLAN, the MAC+IP count is shown as zero. PR1454603
- On QFX5120 switches, untagged hosts ARP/NS requests connected on **encapsulation ethernet-bridge** interface are not being resolved. PR1454804
- You might not be able to apply a firewall filter to a particular Virtual Chassis or Virtual Chassis Fabric member as TCAM is running out of space. PR1455177
- In a 16+ member QFX5100 Virtual Chassis Fabric, the **FROM** column under the **show system users** command output reports feb0, feb1, feb2, and feb3 for fpc16, fpc17, fpc18, and fpc19, respectively. PR1455201
- The priority-based flow control (PFC) feature does not work on the QFX10000 line of switches. PR1455309
- The cosd crash might be observed if the **forwarding-class-set** is directly applied on the child interface of an aggregated Ethernet interface. PR1455357
- Link-up delay and traffic drop might be seen on mixed service provider Layer 2/Layer 3 and enterprise style Layer 2 type configurations. PR1456336

- The Packet Forwarding Engine process might crash after Routing Engine switchover on QFX10000 platforms. PR1457414
- Overtemperature SNMP trap messages are displayed after an update even though the temperatures are within the system thresholds. PR1457456
- On QFX5110 switches, port 51 has one LED blinking amber continuously. PR1457516
- On QFX5210 switches, the LED does not light on port 64 and 65 after the switch is upgraded to Junos OS Release 19.2R1. PR1458514
- The command **show dynamic-tunnels database** does not show **v6 mapped** next-hop flag for 6PE routes that have labels. PR1458634
- The BPDU packet might be looped between leaf DF switch and non-DF switch and causes traffic blocking. PR1458929
- On QFX5200 switches, DHCPv6 LDRA relay bounded count is not as expected after DHCP is configured. PR1459499
- The fxpc process might crash because the BGP IPv6 session flaps. PR1459759
- The **forwarding** option is missed in routing instance type. PR1460181
- The **accept-source-mac** feature with VXLAN is not working on QFX5000 platforms. PR1460885
- The statement **show forwarding-options enhanced-hash-key** is not supported on QFX10000 platforms. PR1462519
- The entPhysicalTable MIB is not fetching expected data on QFX10002-72Q or QFX10002-36Q platforms. PR1462582
- The fxpc process might generate core files when changing MTU in a VXLAN scenario with firewall filters applied on QFX5000 platforms. PR1462594
- On QFX5100 Virtual Chassis or Virtual Chassis Fabric, you observe the **BRCM-VIRTUAL,brcm_vxlan_walk_svp(),6916:Failed to find L2-iff for ifl:** error while cleaning up EVPN-VXLAN configurations with mini-PDT base configurations. PR1463939
- On PTX10000, the FPC might restart during runtime. PR1464119
- On QFX10000 platforms, the interface might not come up on FPC restart. PR1464650
- QFX5100-24Q: Unable to apply DSCP rewrite to firewall filter to a Layer 3 subinterface (for example, xe-0/0/0.100). PR1464883
- PEM is not present spontaneously on QFX5210. PR1465183
- On QFX5100-48T switches, a 10-Gigabit Ethernet interface might not come up or negotiate at speed 1-Gbps when connected with BRCM 10G/GbE 2+2P 57800-t rNDC. PR1465196
- The QSFP-100G-PSM4 could not be correctly identified on QFX5200 or QFX5110 platforms. PR1465214
- The physical interface of an aggregated Ethernet might take time to come up after disabling or enabling it. PR1465302

- Junos OS exhibits inconsistent fan and power supply numbering on White Boxs (-O and -OZ) in Release 19.2R1. PR1465327
- In a Virtual Chassis scenario, the broadcast and multicast traffic might be dropped over an IRB or a LAG interface. PR1466423
- BGP open messages with specific types of BGP optional capabilities causing BMP messages not to be encoded correctly when sent to the BMP collector. PR1466477
- On QFX10000 platforms, EBUF parity interrupt is not seen. PR1466532
- IPv6 traffic over Layer 3 VPN might fail. PR1466659
- Slow packet drops might be seen on QFX5000 platforms. PR1466770
- EPR iCRC errors in QFX10000 platforms might cause protocols to be down. PR1466810
- A few of the DHCPvX INFORM messages, specific to a particular VLAN, are not receiving any ACK from server. PR1467182
- Ingress drops to be included at the CLI from interface statistics and added to InDiscards. PR1468033
- Optics measurements might not be streamed for interfaces of a PIC over JTI. PR1468435
- MAC address might not be learned on a new extended port after VMotion in a Junos fusion for data center environment. PR1468732
- QFX5000 platform is looping the IP routed packet through IS-IS or MPLS. PR1469998
- Incorrect counter values are observed for the arrival rate and peak rate for DDoS commands. PR1470385
- On QFX5100 and EX4300 mixed-mode Virtual Chassis, unable to configure 10-Mbps speed on the Gigabit Ethernet interface. PR1471216
- In a VXLAN scenario on QFX10000 platforms, when a VTEP source interface is configured in multiple routing instances, traffic loss might occur. PR1471465
- On QFX5000 platforms, egress PACL size is half. PR1472206
- The shaping of CoS does not work after reboot. PR1472223
- The detached interface in a LAG might process the xSTP BPDUs. PR1473313
- The RIPv2 packets forwarded across a Layer 2 circuit connection might be dropped. PR1473685
- On QFX5000 platforms in an EVPN-VXLAN scenario, continuous log messages might be observed. PR1474545
- Layer 2 circuit might fail to communicate via VLAN 2 on QFX5000 platforms. PR1474935
- DAC cables are not being properly detected in the Packet Forwarding Engine on QFX5200 switches. PR1475249
- QFX5000 leaf device might fail to forward the traffic in a multicast environment with VXLAN. PR1475430
- QFX Series platform generates the **invalid PFE PG counter pairs to copy, src 0xfffff80, dst 0** message. PR1476829

- On QFX10002-36Q and QFX10002-72Q switches, generating continuous **prds_ptc_wait_adoption_status: PECHIP[1] PTC[1]: timeout on getting adoption valid bit[8] asserted** error logs on the device. PR1477192
- The remaining interface might be still in downstate even the number of channelized interfaces is no more than five. PR1480480
- ARP request packets for unknown hosts might get dropped in a remote PE in an EVPN-VXLAN scenario. PR1480776
- On QFX10000 and QFX5000 Series switches with SP style configuration, BUM traffic incorrectly get blocked, while you disable or enable different logical interfaces. PR1482202
- After an ISSU or an ISSR, a port using SR4 or LR4 optics might not come up. PR1490799

High Availability (HA) and Resiliency

- Unified ISSU is not supported on QFX5000 platforms. PR1472183

Interfaces and Chassis

- VRRPv6 state is flapping with init and idle states after configuring **vlan-tagging**. PR1445370
- Traffic might be forwarded to incorrect interfaces in an MC-LAG scenario. PR1465077
- On a QFX Series platform, VRRPv3 MIBs are not working to poll VRRPv6-related objects. PR1467649
- Executing commit might become unresponsive due to a stuck dcd process. PR1470622
- Commit error is not thrown when a member link is added to multiple aggregation groups with different interface-specific options. PR1475634

Junos Fusion Enterprise

- Loop detection might not work on extended ports in Junos fusion for enterprise scenarios. PR1460209

Junos Fusion Satellite Software

- In Junos fusion for enterprise, dpd might crash on satellite devices running SNOS. PR1460607

Layer 2 Features

- On QFX5100 switches, storm control configuration might be disabled for the interface. PR1354889
- Physical layer and MAC/ARP learning might not work for copper base SFP-T transceivers on QFX5100 and QFX5110. PR1437577

- The LLDP function might fail when a Juniper device connects to a non-Juniper device. PR1462171
- A few MAC addresses might be missing from the software MAC table on QFX5000 platforms. PR1467466
- After rebooting, an FXPC core file might be seen when committing the configuration. PR1467763
- Ingress traffic might be silently dropped if the underlying interface flaps in an EVPN-VXLAN scenario. PR1469596
- Traffic might be affected if composite next hop is enabled. PR1474142

Layer 2 Ethernet Services

- In an EVPN-VXLAN ERB scenario, **dhcp relay-source lo0.1** is not used when enabled with anycast legacy IRB. PR1455076
- Member links state might be asychronized on a connection between PE and CE devices in an EVPN A/A scenario. PR1463791

Multiprotocol Label Switching (MPLS)

- On QFX10002 switches, the **show mpls static-lsp | display xml** command produces invalid XML. PR1469378
- Traffic might silently dropped and discarded on PE when CE sends traffic to PE and the destination is resolved with two LSPs through one upstream interface. PR1475395
- MPLS LDP ping or traceroute fails over QFX5100 as transit PHP node. PR1477301

Platform and Infrastructure

- The stylesheet language alternative syntax (SLAX) script might be lost after upgrading software. PR1479803

Routing Protocols

- In a scaled setup, when the host table is full and the host entries are installed in the LPM table, OSPF sessions might take more time to come up. PR1358289
- Invalid VRRP mastership election on QFX5110 Virtual Chassis peers. PR1367439
- Host-destined packets with **filter log** action might not reach the Routing Engine if log/syslog is enabled. PR1379718
- On QFX5100, BGP IPv4 or IPv6 convergence and RIB install or delete time degraded in Junos OS Releases 19.1R1, 19.2R1, 19.3R1, and 19.4R1. PR1414121

- PIM (S, G) joins can cause MSDP to incorrectly announce source active messages in some cases. PR1443713
- CRC errors might be seen on QFX5100 Virtual Chassis. PR1444845
- The core file might be generated when you add or remove EVPN Type-5 routing instance. PR1455547
- On QFX5000 platforms, egress port for ARP entry in the Packet Forwarding Engine is not modified from the VTEP to the local ESI port, after the device boots up.PR1460688
- On QFX5100 Virtual Chassis or Virtual Chassis Fabric, the **brcm_ipmc_route_counter_delete:3900Multicast stat destroy failed (-10:Operation still running)** error is observed after unified ISSU with Mini-PDT base configurations. PR1460791
- The **other querier present interval** timer cannot be changed in an IGMP/MLD snooping scenario. PR1461590
- When IRB is deleted on the Layer 3 gateway, the IRB interface does not get removed from the Packet Forwarding Engine and it results in traffic drop in IRB MAC address. PR1463092
- The mcsnoopd crash might be seen if one BD/VLAN is configured as part of EVPN and it has any multicast router interfaces (static/dynamic). PR1468737
- Traffic might not be forwarded over an ECMP link in an EVPN-VXLAN scenario. PR1475819
- ARP packets are always sent to CPU regardless of whether the **storm-control** is activated. PR1476708
- GRE transit traffic is not forwarded in a VRRP scenario. PR1477073

SEE ALSO

What's New | **171**

What's Changed | **178**

Known Limitations | **180**

Open Issues | **181**

Documentation Updates | **193**

Migration, Upgrade, and Downgrade Instructions | **194**

Documentation Updates

IN THIS SECTION

- Dynamic Host Configuration Protocol (DHCP) | **194**

This section lists the errata and changes in Junos OS Release 20.1R1 documentation for the QFX Series.

Dynamic Host Configuration Protocol (DHCP)

- **Introducing DHCP User Guide**—Starting in Junos OS Release 20.1R1, we are introducing the DHCP User Guide for Junos OS routing, switching, and security platforms. This guide provides basic configuration details for your Junos OS device as DHCP Server, DHCP client, and DHCP relay agent.

  [See DHCP User Guide.]

SEE ALSO

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.

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 **20.1** in the Release pull-down list to the right of the Software tab on the Download Software page.

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 20.1 release.

   An Alert box appears.

5. In the Alert box, click the link to the PSN document for details about the software, and click the link to download it.

   A login screen appears.

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

7. Download the software to a local host.

8. Copy the software to the device or to your internal software distribution site.

9. Install the new jinstall package on the device.

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

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

`user@host>` **request system software add**
***source*/jinstall-host-qfx-5-x86-64-20.1-R1.n-secure-signed.tgz reboot**

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 20.1 **jinstall** package, you can issue the **request system software rollback** command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

This section explains how to upgrade the software, which includes both the host OS and the Junos OS. This upgrade requires that you use a VM host package—for example, a **junos-vmhost-install-x.tgz** .

During a software upgrade, the alternate partition of the SSD is upgraded, which will become primary partition after a reboot .If there is a boot failure on the primary SSD, the switch can boot using the snapshot available on the alternate SSD.

> **NOTE:** The QFX10002-60C switch supports only the 64-bit version of Junos OS.

> **NOTE:** If you have important files in directories other than /config and /var, copy the files to a secure location before upgrading. The files under /config and /var (except /var/etc) are preserved after the upgrade.

To upgrade the software, you can use the following methods:

If the installation package resides locally on the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-20.1R1.9.tgz
```

If the Install Package resides remotely from the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add
ftp://ftpserver/directory/junos-vmhost-install-qfx-x86-64-20.1R1.9.tgz
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Installing the Software on QFX10002 Switches

NOTE: If you are upgrading from a version of software that does not have the FreeBSD 10 kernel (15.1X53-D30, for example), you will need to upgrade from Junos OS Release 15.1X53-D30 to Junos OS Release 15.1X53-D32. After you have installed Junos OS Release 15.1X53-D32, you can upgrade to Junos OS Release 15.1X53-D60 or Junos OS Release 18.3R1.

NOTE: On the switch, use the **force-host** option to force-install the latest version of the Host OS. However, by default, if the Host OS version is different from the one that is already installed on the switch, the latest version is installed without using the **force-host** option.

If the installation package resides locally on the switch, execute the **request system software add *<pathname><source>* reboot** command.

For example:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-f-x86-64-20.1R1.n-secure-signed.tgz reboot
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* reboot** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-f-x86-64-20.1R1.n-secure-signed.tgz reboot
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

The switch contains two Routing Engines, so you will need to install the software on each Routing Engine (re0 and re1).

If the installation package resides locally on the switch, execute the **request system software add *<pathname><source>*** command.

To install the software on re0:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* re0** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

To install the software on re1:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* re1** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

Reboot both Routing Engines.

For example:

```
user@switch> request system reboot both-routing-engines
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Installing the Software on QFX10008 and QFX10016 Switches

Because the switch has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

WARNING: If graceful Routing Engine switchover (GRES), nonstop bridging (NSB), or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you issue the CLI **delete chassis redundancy** command when prompted. If GRES is enabled, it will be removed with the **redundancy** command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the **[edit routing-options]** hierarchy level to disable it.

1. Log in to the master Routing Engine's console.

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

2. From the command line, enter configuration mode:

   ```
   user@switch> configure
   ```

3. Disable Routing Engine redundancy:

   ```
   user@switch# delete chassis redundancy
   ```

4. Disable nonstop-bridging:

   ```
   user@switch# delete protocols layer2-control nonstop-bridging
   ```

5. Save the configuration change on both Routing Engines:

   ```
   user@switch# commit synchronize
   ```

6. Exit the CLI configuration mode:

   ```
   user@switch# exit
   ```

After the switch has been prepared, you first install the new Junos OS release on the backup Routing Engine, while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the software version on the other Routing Engine.

7. Log in to the console port on the other Routing Engine (currently the backup).

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

8. Install the new software package using the **request system software add** command:

   ```
   user@switch> request system software add validate
   /var/tmp/jinstall-host-qfx-10-f-x86-64-20.1R1.n-secure-signed.tgz
   ```

   For more information about the **request system software add** command, see the CLI Explorer.

9. Reboot the switch to start the new software using the **request system reboot** command:

   ```
   user@switch> request system reboot
   ```

   > **NOTE:** You must reboot the switch to load the new installation of Junos OS on the switch.
   >
   > To abort the installation, do not reboot your switch. Instead, finish the installation and then issue the **request system software delete *<package-name>*** command. This is your last chance to stop the installation.

   All the software is loaded when you reboot the switch. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

   While the software is being upgraded, the Routing Engine on which you are performing the installation is not sending traffic.

10. Log in and issue the **show version** command to verify the version of the software installed.

    ```
    user@switch> show version
    ```

    Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the master Routing Engine software.

11. Log in to the master Routing Engine console port.

    For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

12. Transfer routing control to the backup Routing Engine:

    ```
    user@switch> request chassis routing-engine master switch
    ```

    For more information about the **request chassis routing-engine master** command, see the CLI Explorer.

13. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

    ```
    user@switch> show chassis routing-engine
    Routing Engine status:
      Slot 0:
        Current state                  Backup
        Election priority              Master (default)
    Routing Engine status:
      Slot 1:
        Current state                  Master
        Election priority              Backup (default)
    ```

14. Install the new software package using the **request system software add** command:

    ```
    user@switch> request system software add validate
    /var/tmp/jinstall-host-qfx-10-f-x86-64-20.1R1.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 205
- Upgrading the Software Using Unified ISSU on page 205

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-x86-64-20.1R1.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 17.1, 17.2 and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

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

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

SEE ALSO

- What's New | 171
- What's Changed | 178
- Known Limitations | 180
- Open Issues | 181
- Resolved Issues | 186
- Documentation Updates | 193

Junos OS Release Notes for SRX Series

IN THIS SECTION

These release notes accompany Junos OS Release 20.1R1 for the SRX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

Application Security

- **Custom application enhancements (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 20.1R1, we've enhanced the custom applications signature functionality by providing a new set of applications and contexts.

  Application identification allows you to create custom application signatures to detect applications specific to your network environment. You can create custom application signatures for applications based on ICMP, IP protocol, IP address, and Layer 7 or TCP/UDP stream. While configuring the custom application signatures, you must specify the context values that the device can use to match the patterns in the application traffic.

  Custom application signature contexts are part of application signature package. You must download and install the latest application signature package version 3248 or later to use new contexts for custom application signatures.

  [See Custom Application Signatures for Application Identification.]

- **Default mechanism to forward the traffic through APBR rule (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS 20.1R1, you can configure a APBR rule by specifying the dynamic application match criteria with any keyword. This provides a default mechanism to forward the traffic to a specific next-hop device or to a destination if the traffic matches any dynamic application.

  [See Advanced Policy-Based Routing.]

- **AppQoE support for granular APBR rules (NFX Seris, SRX Series, and vSRX)**—Starting in Junos OS Release 20.1R1, AppQoE utilizes the granular rule matching functionality of advanced policy-based routing (APBR) for better quality of experience (QoE) for the application traffic.

  In Junos OS Release 18.2R1, APBR supported configuring policies by defining source addresses, destination addresses, and applications as match conditions. After a successful match, the configured APBR profile is applied as an application services for the session. In this release, AppQoE leverages the APBR enhancement and selects the best possible link for the application traffic as sent by APBR to meet the performance requirements specified in SLA.

  [See Application Quality of Experience.]

Authentication and Access Control

- **Support for UPN as user identity (SRX Series)**—Starting in Junos OS Release 20.1R1, you can use User Principal Name (UPN) as logon name in firewall-authentication, which is working as a captive portal for JIMS or user-firewall.

  You can use UPN as logon name along with *cn* or *sAMAccountName* at the same time. UPN can be used instead of *sAMAccountName* to authenticate a user.

  Even if user uses UPN as logon name, firewall authentication pushes *sAMAccountName* (mapping to the UPN) to user ID rather than pushing the UPN.

Firewall-authentication pushes both UPN and *sAMAccountName* (mapping to the UPN) to JIMS.

[See Understanding Advanced Query Feature for Obtaining User Identity Information from JIMS.]

- **Trusted Platform Module (TPM) to bind secrets (SRX5400, SRX5600, and SRX5800)**—Starting with Junos OS Release 20.1R1, we've introduced the TPM support on the SRX5000 line of devices with SRX5K-RE3-128G Routing Engine (RE3). The TPM chip is enabled by default to make use of TPM functionality.

  When TPM is activated, it protects the private keys stored in Junos OS.

  [See Using Trusted Platform Module to Bind Secrets on SRX Series Devices.]

Flow-Based and Packet-Based Processing

- **Support of IPFIX formatting and Chassis Cluster for SRX J-Flow functionality (SRX300, SRX320, SRX340, SRX345, and SRX550HM)** —Starting with Junos OS Release 20.1R1, you can configure Chassis Cluster and define an IPFIX flow record template suitable for IPv4 traffic or IPv6 traffic. IPFIX is an enhanced version of J-flow version 9 template. Using IPFIX, you can collect a set of sampled flows and send the record to a specified host.

  See [Configuring Flow Aggregation to Use IPFIX Flow Templates on MX, vMX and T Series Routers, EX Series Switches, and SRX devices.]

- **Support service inspection for pass-through IP-IP and GRE tunnel in TAP mode (SRX300, SRX320, SRX340, SRX345, SRX1500, SRX4100, and SRX4200)**—Starting in Junos OS Release 20.1R1, TAP mode inspects IP-IP and GRE inner tunnel traffic by de-encapsulating the outer and inner IP header (up to two levels) to create flow sessions. You can configure up to eight TAP interfaces on an SRX Series device.

  [See TAP Mode for Flow Sessions, and forwarding-options.]

GPRS

- **Increase in GTP scale for IoT and roaming firewall applications (SRX1500, SRX4100, SRX4200, and vSRX)**—Starting in Junos OS Release 20.1R1, in addition to the existing support on SRX5400, SRX5600, SRX5800, and SRX4600, to enable the Internet of Things (IoT) and roaming firewall use cases, the GTP tunnel scale is increased for the following SRX Series devices:
  - SRX1500: 204,800 to 1,024,000
  - SRX4100: 409,600 to 4,096,000
  - SRX4200: 819,200 to 4,096,000

  For vSRX instances, the number of tunnels supported depends on the available system memory.

[See Understanding Policy-Based GTP.]

Hardware

- **SRX380 Services Gateway**—The SRX380 Services Gateway is a high performance and all-in-one networking device, which consolidates routing, switching, and security. With next-generation firewall features and advanced threat mitigation capabilities, the SRX380 device provides cost-effective and secure connectivity across distributed enterprise locations. A 1U form factor model with a 16-core MIPS processor and 4-GB DDR4 RAM, the SRX380 device supports up to 10-Gbps firewall performance.

  The SRX380 device has an integrated 100-GB SSD and provides high port density with 16 on-board PoE-enabled 1-Gigabit Ethernet RJ-45 ports and 4 10-Gigabit Ethernet SFP+ ports. All the ports support AES-256 MACsec encryption. The SRX380 device has dual AC power supplies and supports up to four Mini-PIMs.

  The SRX380 supports the same features as those supported on the existing SRX300 line of services gateways. For the complete list of features supported on the SRX380, see Feature Explorer.

  [See SRX380 Services Gateway Overview.]

Interfaces and Chassis

- **Support for new show | display set CLI commands (ACX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the following new **show** commands have been introduced:
  - **show | display set explicit**—Display explicitly, as a series of commands, all the configurations that the system internally creates when you configure certain statements from the top level of the hierarchy.
  - **show | display set relative explicit**—Display explicitly, as a series of commands, all the configurations that the system internally creates when you configure certain statements from the current hierarchy level.

  [See show | display set and show | display set relative.]

Intrusion Detection and Prevention

- **HTTP X-Forwarded-For header support in IDP (SRX Series)**—Starting from Junos OS Release 20.1R1, we've introduced the **log-xff-header** option to record the x-forward-for header (xff-header) information. When this option is enabled. During the traffic flow, IDP saves the source IP addresses (IPv4 or IPv6) from the contexts for HTTP and SMTP traffics and displays in attack logs.

  The xff-header is not processed unless its enabled through sensor-configuration.

  - To enable the xff-header, use the **set security idp sensor-configuration global log-xff-header** command.

- To disable the xff-header, use the **delete security idp sensor-configuration global log-xff-header** command.

Previously, when you access internet, to lessen the external bandwidth the servers used transparent proxies. It was difficult to identify the originating source IP address as the proxy server converted it into an anonymous source IP address.

[See Understanding Multiple IDP Detector Support.]

Juniper Sky ATP

- **Juniper Sky ATP support for disabling standard Juniper C&C and URL feeds**—Starting in Junos OS Release 20.1R1, you can disable standard Juniper command and control (C&C) and URL feeds on SRX Series devices. Disabling the Juniper C&C and URL feeds helps to free the resources on SRX Series devices and makes the resources available for loading custom feeds. Use the **set services security-intelligence disable-global-feed (all | feed name *feed-name*)** command to disable the feeds. To enable the feeds, use the **delete services security-intelligence disable-global-feed (all | feed name *feed-name*)** command.

  [See set services security-intelligence and show services security-intelligence category summary.]

Junos OS XML API and Scripting

- **The jcs:load-configuration template supports loading the rescue configuration (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the **jcs:load-configuration** template supports the **rescue** parameter to load and commit the rescue configuration on a device. SLAX and XSLT scripts can call the **jcs:load-configuration** template with the **rescue** parameter set to **"rescue"** to replace the active configuration with the rescue configuration.

  [See Changing the Configuration Using SLAX and XSLT Scripts and jcs:load-configuration Template.]

J-Web

- **J-Web supports SRX380 device**—Starting in Junos OS Release 20.1R1, you can use J-Web to manage your SRX380 device. Additionally, you can also:
  - Monitor wireless LAN setting of the supported Wi-Fi Mini-PIM: Monitor > Wireless LAN.
  - View power statistics information using the new Power Budget Statistics tab: Monitor > Chassis Information > Chassis Component Details.

    NOTE: You can view the power statistics information only when the device is in standalone mode.

- Configure wireless LAN setting of the supported Wi-Fi Mini-PIM: Configure > Wireless LAN > Settings.
- Configure redundant power supply for power management using the new Redundant PSU menu: Configure > Basic Settings.

[See Dashboard Overview, Monitor Wireless LAN, and About the Settings Page.]

Network Management and Monitoring

- **SNMP support to export statistics of user firewall (SRX Series and vSRX)**—Starting in Junos OS Release 20.1R1, the new MIB jnxUserFirewalls OID is introduced to expose statistics of user firewall identity-management counters to network monitoring tools supporting SNMP.

  [See Enterprise-Specific SNMP MIBs Supported by Junos OS.]

- **SNMP support to monitor Express Path status (SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 20.1R1, the new SNMP MIB jnxJsFlowSofSummary is introduced to improve the Express Path mode (formerly known as services offloading) session status using CLI monitoring and traffic logging. The jnxJsFlowSofSummary MIB Provides the total number of Express Path sessions in use and total number of packets processed so far in the logical system.

  [See Enterprise-Specific SNMP MIBs Supported by Junos OS.]

- **Enhanced PKI traps, log notifications, and SNMP for IPsec VPN (MX Series with USF and the SRX5000 line of devices with SPC3 card)**—Starting in Junos OS Release 20.1R1, you can enable the peer down and IPsec tunnel down traps and configure the certificate authority (CA) and local certificate traps. We've enhanced the existing IPsec VPN flow monitor MIB **jnxIpSecFlowMonMIB** to support the global data plane, active IKE SA, active IPsec SA, and active peer statistics for tunnels using IKEv2. We've also enhanced the output of the **show security ike stats** command to add additional options **(<brief> | <detail>)**. Use the **clear security ike stats** command to clear the IKEv2 statistic counters.

  [See Configure the Certificate Expiration Trap, Enterprise-Specific SNMP MIBs Supported by Junos OS, Enable Peer Down and IPsec Tunnel Down Traps, trap (Security PKI), trap (Security IKE), clear security ike stats, show security ike stats, show security ipsec statistics, show security ike security-associations, and show security ike active-peer.]

Port Security

- **Media Access Control Security (MACsec) support (SRX380)**—SRX380 supports MACsec in on all 16 1GbE ports and all four 10GbE ports. MACsec is an industry-standard security technology that provides secure communication for all traffic on point-to-point Ethernet links. The supported cipher suites are GCM-AES-256 and GCM-AES-128. Only static CAK mode is supported.

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

Security

- **Support for security policy reports (SRX Series and vSRX)**—Starting in Junos OS Release 20.1R1, you can use the **show security policy-report** command to display detailed security policy reports.

  Optimizing security policies ensure that the policies are efficient. Over time, policies become disorganized and hence ineffective. You can use the **show security policy-report** command to notify end users when you create new policies or change existing policies that adversely affect other security policies.

  You can use the **report-skip** command at the **[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name*]** hierarchy level to exclude the policy from the policy analysis and prevent it from appearing in any future report.

  [See show security policy-report and report-skip.]

- **Support to clear DNS cache if DNS error responses are received (SRX Series and vSRX)**—Starting in Junos OS Release 20.1R1, you can clear the DNS cache entry IP list when DNS error responses are received. We have introduced a new command, **dns-cache** under the **[edit security policies]** hierarchy level, to configure the security policy DNS cache behavior.

  [See dns-cache.]

System Management

- **Restrict option under NTP configuration is now visible (ACX Series, QFX Series, MX Series, PTX Series, and SRX Series)**—Starting in Junos OS Release 20.1R1, the **noquery** command under the **restrict** hierarchy is now available and can be configured with a mask address. The **noquery** command is used to restrict ntpq and ntpdc queries coming from hosts and subnets.

  [See Configuring NTP Access Restrictions for a Specific Address.]

Tenant Systems and Logical Systems

- **ICAP service redirect support for tenant systems (SRX Series and vSRX)**—You can prevent data loss from your network by employing Internet Content Adaptation Protocol (ICAP) redirect services. Starting

in Junos OS Release 20.1R1, you can enable ICAP at the tenant system level, and you can view/clear the ICAP services redirect status and statistics at the tenant systems level.

In addition, we've introduced the **X-Client-IP**, **X-Server-IP**, **X-Authenticated-User**, and **X-Authenticated-Groups** header extensions in an ICAP message to provide information about the source of the encapsulated HTTP message.

[See ICAP Service Redirect and icap-redirect.]

- **Express Path session status CLI monitoring improvement and traffic logging (SRX4600, SRX5400, SRX5600, and SRX5800)**—The Express Path (formerly known as services offloading) support is already available on SRX4600, SRX5400, SRX5600, and SRX5800 Series devices. Express Path considerably reduces packet-processing latency. Starting in Junos OS Release 20.1R1, you can view the total number of services-offload sessions and total number of services-offload packets processed in the CLI. In addition, you can configure the services-offload traffic logging at the logical system and tenant system level.

  [See Express Path.]

VPNs

- **Common configuration payload password support for RADIUS server (SRX Series and vSRX)**—Starting in Junos OS Release 20.1R1, you can configure a common password for IKEv2 configuration payload requests for an IKE gateway configuration. The common password in the range of 1 to 128 characters allows the administrator to define a common password. This password is used when the SRX Series device is requesting an IP address on behalf of a remote IPsec peer using IKEv2 configuration payload over the RADIUS server. The RADIUS server matches the credentials before it assigns any IP information to the configuration payload request.

  [See Understanding IKEv2 Configuration Payload.]

SEE ALSO

What's Changed | 217

Known Limitations | 220

Open Issues | 222

Resolved Issues | 223

Documentation Updates | 229

Migration, Upgrade, and Downgrade Instructions | 230

What's Changed

IN THIS SECTION

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

ALG

- **Disable the do not fragment flag from packet IP header (SRX Series and vSRX)**—Starting in Junos OS Release 20.1R1, we've introduced the **clear-dont-frag-bit** option at the [**edit security alg alg-manager**] hierarchy level to disable the do not fragment flag from the packet IP header, which allows the packet to be split after NAT is performed.

  In Junos OS releases earlier than Release 20.1R1, when the ALG performs payload-NAT, sometimes the size of the packet becomes bigger than the outgoing interface maximum transmission unit (MTU). If the packet IP header has the do not fragment flag, this packet cannot be sent out.

  [See alg-manager.]

Application Security

- Starting in Junos OS Release 20.1R1, you can enable application identification (AppID) to classify a web application that is hosted on a content delivery network (CDN) such as AWS, Akamai, Azure, Fastly, and Cloudflare and so on accurately. Use the following configuration statement to enable CDN application classification:

  ```
  [edit]
  user@host# user@hots# set service application-identification enable-cdn-application-detection
  ```

  When you apply the configuration, AppID identifies and classifies actual applications that are hosted on the CDN.

[See Application Identification]

- You can configure maximum memory limit for the deep packet inspection (DPI) by using the following configuration statement:

  ```
  user@host# set services application-identification max-memory memory-value
  ```

  You can set 1 through 200000 MB as memory value.

  Once the JDPI memory consumption reaches to 90% of the configured value, then DPI stops processing new sessions.

  [See Application Identification]

- Starting in Junos OS Release 20.1R1, you can configure and use IP protocol-based custom application signatures on your SRX Series device. In previous versions of Junos OS Releases from 19.2 through 19.4 release, IP protocol based custom application signatures did not work as expected.

  In Junos OS Releases in 19.2 through Junos OS Releases 19.4 and their maintenance releases, IP protocol based custom application signatures do not work as expected. As a workaround, you can configure the IP protocol-based applications at the following hierarchy levels:

  - For unified policy: Use service based application configuration as below:

    ```
    user@host# set applications application application-name protocol IP -proto-number
    ```

  - For legacy application firewall: Use predefined IP protocol applications as below:

    ```
    user@host# set security application-firewall rule-sets rule-set-name rule rule-name match dynamic-application
      junos:IPP-IGMP
    ```

  [See Custom Application Signatures for Application Identification.]

Ethernet Switching and Bridging

- **LLDP support on redundant Ethernet interfaces (SRX Series)**—Starting in Junos OS Release 20.1R1, you can configure the Link Layer Discovery Protocol (LLDP) on redundant Ethernet (reth) interfaces. Use the **set protocol lldp interface *<reth-interface>*** command to configure LLDP on the reth interface.

  [See Configuring LLDP and Ethernet Ports Switching Overview for Security Devices.]

J-Web

- Deactivated policy rules are not visible in the J-Web UI (SRX Series)—J-Web does not support disabling or enabling the security firewall or global policy rules from Junos OS Release 19.4R1. The policy rules that are deactivated through CLI are also not visible in the J-Web UI. As a workaround, use CLI to disable or enable the policy rules on the device.

Unified Threat Management (UTM)

- **Increase in the UTM scale number (SRX1500, SRX4100, SRX4200, SRX4600, SRX4800, SRX5400, SRX5600, and SRX5800)**—Starting with Junos OS Release 20.1R1, on SRX Series devices, UTM policies, profiles, MIME patterns, filename extensions, protocol commands, and custom messages are increased up to 1500. Custom URL patterns and custom URL categories are increased up to 3000.

  [See Unified Threat Management overview.]

VPNs

- **Public key infrastructure warning message (SRX Series)**—Starting in Junos OS Release 20.1R1, a warning message **ECDSA Keypair not supported with SCEP for cert_id *<certificate id>*** is displayed when you try to enroll a local certificate using an Elliptic Curve Digital Signature Algorithm (ECDSA) key with Simple Certificate Enrollment Protocol (SCEP) because ECDSA key is not supported with SCEP.

  Prior to Junos OS Release 20.1R1, the warning message is not displayed.

  [See Example: Enrolling a Local Certificate Online Using SCEP.]

- **Change in display of local certificate serial number (SRX Series)**—In Junos OS Release 20.1R1, the output of the **show security pki local-certificate detail** command is modified to display the PKI local certificate serial number with **0x** as prefix to indicate that the PKI local certificate is in the hexadecimal format.

  [See show security pki local-certificate (View).]

SEE ALSO

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for SRX Series.

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

J-Web

- When a dynamic application is created for an edited policy rule, the list of services will be blank when the services tab is clicked and then the policy grid will be autorefreshed. As a workaround, create a dynamic application as the last action while modifying the policy rule and click the Save button to avoid loss of configuration changes made to the policy rule. PR1460214

Platform and Infrastructure

- On an SRX4600 device, when LLDP is configured on the interfaces, Packet Forwarding Engine stops are seen due to the segmentation problem. LLDP is not supported on SRX4600 currently, but can be configured. PR1422466

VPNs

- On SRX5400, SRX5600, and SRX5800 devices with an SPC3 card, with 60,000 tunnels up, when RG0 failover happens while an IPsec and/or IKE rekey is in progress, those rekeying tunnels might go down and traffic loss might be seen until the tunnel is reestablished. PR1471499
- In SPC2 and SPC3 mixed mode HA deployments, tunnel per second (TPS) is getting affected while dead peer detection (DCD) 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

SEE ALSO

What's New | **209**

What's Changed | **217**

Open Issues | **222**

Resolved Issues | **223**

Documentation Updates | **229**

Migration, Upgrade, and Downgrade Instructions | **230**

Open Issues

IN THIS SECTION

Learn about open issues in this release for SRX Series.

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

Flow-Based and Packet-Based Processing

- A maximum of 250 Web proxy profile creations are supported on all SRX Series devices. PR1428495

Platform and Infrastructure

- On SRX1500 and the SRX4000 line of devices, physically disconnecting the cable from fxp0 interface causes hardware monitor failure and redundancy group failover, when the device is the primary node in a chassis cluster. PR1467376

Routing Policy and Firewall Filters

- If a huge number of policies are configured on SRX Series devices and some policies are changed, the traffic that matches the changed policies might be dropped. PR1454907
- On SRX5400, SRX5600, and SRX5800 devices, on reth interfaces that are configured as DHCP clients, after a reboot of the device the interface might not get an IP address when you use the default number of DHCP retransmission attempts. When the number of retransmission attempts is increased to 5 or higher, it works fine. PR1458490

VPNs

- On the SRX5000 line of devices with SPC3 cards, sometimes IKE SA is not seen on the device when st0 binding on VPN configuration object is changed from one interface to another (for example, st0.x to st0.y). PR1441411
- With NCP remote access solution, in a PathFinder case (for example, where IPsec traffic has to be encapsulated as TCP packets), TCP encapsulation for transit traffic is failing. PR1442145
- On the SRX5000 line of devices with SPC3 and SPC2 mixed mode, with a very large amount of IKE peers (60,000) with dead peer detection (DPD) enabled, IPsec tunnels might flap in some cases when IKE and IPsec rekeys are happening at the same time. PR1473523

SEE ALSO

What's New | 209

What's Changed | 217

Known Limitations | 220

Resolved Issues | 223

Documentation Updates | 229

Migration, Upgrade, and Downgrade Instructions | 230

Resolved Issues

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.

Application Layer Gateways (ALGs)

- Packet's IP header have DF flag might be dropped by SRX Series ALG after payload-NAT. PR1444068
- On the SRX5000 line of devices, the H323 call with NAT64 could not be established. PR1462984
- RTSP data sessions are cleared unexpectedly during cold sync. PR1468001
- The flowd or srxpfe process might stop when an ALG creates a gate with an incorrect protocol value. PR1474942
- SIP messages that need to be fragmented might be dropped by SIP ALG. PR1475031

Authentication and Access Control

- Same-source IP sessions are cleared when the IP entry is removed from the UAC table. PR1457570

Chassis Clustering

- IP monitoring might fail on the secondary node. PR1468441
- An unhealthy node might become primary in SRX4600 devices with chassis cluster scenario. PR1474233

Flow-Based and Packet-Based Processing

- The **trusted-ca** and **root-ca** names or IDs should not be the same within an SSL proxy configuration. PR1420859
- Packet loss is caused by FPGA back pressure on SPC3. PR1429899
- Control logical interface is not created by default for LLDP. PR1436327
- Security logs cannot be sent to the external syslog server through TCP. PR1438834
- The SPC card might stop on the SRX5000 line of devices. PR1439744
- Flowd process core files are generated in the device while testing NAT PBA in AA mode. PR1443148
- The SSL-based AppID simplification effort (removal of HTTPS, POP3S, IMAPS, SMTPS). PR1444767
- In the BERT test for E1 interface, bits counts number is not within the range. PR1445041
- The flowd process might stop on SRX Series devices when chassis cluster and IRB interface are configured. PR1446833
- The AAWM policy rules for IMAP traffic sometimes might not get applied when passed through SRX Series devices. PR1450904
- Introduction of default inspection limits for application identification to optimize CPU usage and improve resistance to evasive applications. PR1454180
- The SRX Series devices stop and generate several core files. PR1455169
- When you try to reset the system configuration on an SRX1500 device using the reset config button, it does not work properly. PR1458323
- The security flow traceoptions fills in with RTSP ALG-related information. PR1458578
- Optimizations were made to improve the connections-per-second performance of SPC3. PR1458727
- LTE dual CPE support with mPIMs when modem receives disconnect event from ISP, need to increase wait timer. PR1460102
- The **security-intelligence** CC feed does not block HTTPS traffic based on SNI. PR1460384

- The AAMWD process exceeds 85 percent RLIMIT_DATA limitation due to memory leak. PR1460619
- Added command to clear specified associated client. PR1461577
- The srxpfe or flowd process might stop if the sampling configuration is changed. PR1462610
- The tunnel packets might be dropped because the gr0.0 or st0.0 interface is wrongly calculated after a GRE or VPN route change. PR1462825
- Fragmented traffic might get looped between the fab interface in a rare case. PR1465100
- TCP session might not time out properly upon receiving TCP RESET packet. PR1467654
- A core file might be generated when you perform an ISSU on SRX Series devices. PR1463159
- The PKI daemon keeps leaking memory on SRX Series devices. PR1465614
- HTTP block message stops working after SNI check for HTTPS session. PR1465626
- Loading CA certificate causes PKI daemon core file to be generated. PR1465966
- The jbuf process usage might increase up to 99 percent after Junos OS upgrade. PR1467351
- The rpd process might stop after several changes to the **flow-spec** routes. PR1467838
- Packet Forwarding Engine might generate core files because SSL proxy is enabled on NFX Series and SRX Series devices. PR1467856
- Server unreachable is detected; ensure that port 443 is reachable. PR1468114
- Tail drop on all ports is observed when any switch-side egress port gets congested. PR1468430
- FTP data connection might be dropped if SRX Series devices send the FTP connection traffic through the dl interface. PR1468570
- RPM test probe fails to show that round-trip time has been exceeded. PR1471606
- Look up failure for expected e-mail address in DUT. PR1472748
- Stateful firewall rule configuration deletion might lead to memory leak. PR1475220
- The **dfs-off** function is enabled. PR1475294
- The nsd process pause might be seen during device reboots if dynamic application groups are configured in policy. PR1478608
- The **show mape rule statistics** command might display negative values. PR1479165
- Sometimes multiple flowd core files are generated on both nodes of chassis cluster at the same time when changing media MTU. PR1489494

Interfaces and Chassis

- The number of mgd processes increases because the mgd processes are not closed properly. PR1439440
- Static route through dl0.0 interface is not active. PR1465199

- MAC limiting on Layer 3 routing interfaces does not work. PR1465366

Intrusion Detection and Prevention (IDP)

- SNMP queries might cause **commit** or **show** command to fail due to IDP PR1444043
- Updating the IDP security package offline might fail in SRX Series devices. PR1466283

J-Web

- The default log query time in J-Web monitoring functionality has been reduced. This increases the responsiveness of the landing pages. PR1423864
- Editing destination NAT rule in J-Web introduces a nonconfigured routing instance field. PR1461599
- The Go button within the J-Web Monitor>Events view now correctly refreshes the logs even when using a blank search query. PR1464593
- J-Web security resources dashboard widget was not being populated correctly. PR1464769

Layer 2 Ethernet Services

- The metric is not changing when configured under the DHCP. PR1461571

Network Address Translation (NAT)

- The flowd or srxpfe process might stop when traffic is processed by both ALGs and NAT. PR1471932
- Issuing the **show security nat source paired-address** command might return an error. PR1479824

Network Management and Monitoring

- The flowd or srxpfe process might stop immediately after committing the jflowv9 configuration or after upgrading to affected releases. PR1471524
- SNMP trap coldStart agent-address becomes 0.0.0.0. PR1473288

Platform and Infrastructure

- Modifying the REST configuration might cause the system to become unresponsive. PR1461021
- VM core files might be generated if the configured sampling rate is more than 65,535. PR1461487

- On the SRX300 line of devices, you might encounter Authentication-Table loading slowly while using user-identification. PR1462922
- The AE interface cannot be configured on an SRX4600 device. PR1465159
- On SRX Series devices, Packet Forwarding Engine memory might be used up if the security intelligence feature is configured. PR1472926
- Support LLDP protocol on reth interface. PR1473456
- Certificate error while configuration validation during Junos OS upgrade. PR1474225
- Packet drop might be observed on the SRX300 line of devices when adding or removing an interface from MACsec. PR1474674
- The commands **request system power-off** and **request system halt** might not work correctly. PR1474985
- The flowd process core files might be seen when there are mixed NAT-T traffic or non-NAT-T traffic with PMI enabled. PR1478812
- When SRX5K-SPC3s or MX-SPC3s are installed in slots 0 or 1 in SRX5800 or MX960 devices, EMI radiated emissions are observed to be higher than regulatory compliance requirements. PR1479001
- The RGx might fail over after RG0 failover in a rare case. PR1479255
- The wl- interface stays in ready status after you execute **request chassis fpc restart** command in Layer 2 mode. PR1479396
- Recent changes to JDPI's classification mechanism caused a considerable performance regression (more than 30 percent). PR1479684
- The flowd or srxpfe process might crash when advanced anti-malware services are used. PR1480005

Routing Policy and Firewall Filters

- Security policies cannot synchronize between Routing Engine and Packet Forwarding Engine on SRX Series devices. PR1453852
- Traffic log shows wrong custom-application name when the **alg ignore** option is used in application configuration. PR1457029
- The NSD process might get stuck and cause problems. PR1458639
- Some domains are not resolved by the SRX Series devices when using DNS address book. PR1471408
- The count option in security policy does not take effect even if the policy count is enabled. PR1471621
- Support for dynamic tunnels on SRX Series devices was mistakenly removed. PR1476530

Routing Protocols

- SSH login might fail if a user account exists in both local database and RADIUS or TACACS+. PR1454177

- The rpd might stop when both instance-import and instance-export policies contain as-path-prepend action. PR1471968

Unified Threat Management (UTM)

- Increase the scale number of UTM profile or policy for the SRX1500 device, and the SRX4000 and SRX5000 lines of devices. PR1455321
- The utmd process might pause after deactivating UTM configuration with predefined category upgrading used. PR1478825

VLAN Infrastructure

- ISSU failed from Junos OS Release 18.4R2.7 to Junos OS Release 19.4, with secondary node PICs in present state after upgrading to Junos OS Release 19.4. PR1468609

VPNs

- IPsec SA inconsistent on SPCs of node0 and node1 in SRX Series devices with chassis cluster. PR1351646
- After RG1 failover, IKE phase 1 SA is getting cleared. PR1352457
- IPsec VPN missing half of the IKE SA and IPsec SA showing incorrect port number when scaling to 1000 IKEv1 AutoVPN tunnels. PR1399147
- The IKE and IPsec configuration under groups is not supported. PR1405840
- The established tunnels might remain unchanged when an IKE gateway is changed from AutoVPN to Site-to-Site VPN. PR1413619
- The VPN tunnel might flap when IKE and IPsec rekey happen simultaneously. PR1421905
- Old tunnel entries might be observed in the output of show security IPsec or IKE SA. PR1423821
- The **show security ipsec statistics** command output displays buffer overflow and wraps around 4,---,---,--- count. PR1424558
- Tunnel does not come up after changing configurations from IPv4 to IPv6 tunnels in the script with gateway lookup failed error. PR1431265
- P1 configuration delete message is not sent on loading baseline configuration if there has been a prior change in VPN configuration. PR1432434
- After a long time (a few hours) of traffic during a mini PDT test, the number of IPsec tunnels is much higher than expected. PR1449296
- Some IPsec tunnels flap after RGs failover on the SRX5000 line of devices. PR1450217
- IPsec VPN flaps if more than 500 IPsec VPN tunnels are connected for the first time. PR1455951

- Traffic is not sent out through an IPsec VPN after update to Junos OS Release 18.2 or later. PR1461793
- On SRX5400, SRX5600, and SRX5800 devices with an SPC3 card, with IKEv1 enabled IKE, the daemon might generate a core file, when IKESA is expired and IPsec tunnel associated with the expired IKESA exists in case of an RG0 failover. Daemon recovers eventually. PR1463501
- The IPsec VPN tunnels cannot be established if overlapped subnets are configured in traffic selectors. PR1463880
- IPsec tunnels might lose connectivity on SRX Series devices after chassis cluster failover when using AutoVPN point-to-multipoint mode. PR1469172
- IPsec tunnels might flap when one secondary node is coming online after reboot in SRX Series high availability environment. PR1471243
- The kmd process might crash continually after the chassis cluster failover in the IPsec ADVPN scenario. PR1479738

SEE ALSO

What's New | **209**

What's Changed | **217**

Known Limitations | **220**

Open Issues | **222**

Documentation Updates | **229**

Migration, Upgrade, and Downgrade Instructions | **230**

Documentation Updates

IN THIS SECTION

- Dynamic Host Configuration Protocol (DHCP) | **230**

Dynamic Host Configuration Protocol (DHCP)

- **Introducing DHCP User Guide**—Starting in Junos OS Release 20.1R1, we are introducing the DHCP User Guide for Junos OS routing, switching, and security platforms. This guide provides basic configuration details for your Junos OS device as DHCP Server, DHCP client, and DHCP relay agent.

  [See DHCP User Guide.]

SEE ALSO

What's New | 209

What's Changed | 217

Known Limitations | 220

Open Issues | 222

Resolved Issues | 223

Migration, Upgrade, and Downgrade Instructions | 230

Migration, Upgrade, and Downgrade Instructions

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

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

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 15.1X49, 17.3, 17.4, 18.1, and 18.2 are EEOL releases. You can upgrade from one Junos OS Release to the next release or one release after the next release. For example you can upgrade from Junos OS Release 15.1X49 to Release 17.3 or 17.4, Junos OS Release 17.4 to Release 18.1 or 18.2, and from Junos OS Release 18.1 to Release 18.2 or 18.3 and so on.

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

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

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

For information about ISSU, see the Chassis Cluster User Guide for Security Devices.

SEE ALSO

- What's New | 209
- What's Changed | 217
- Known Limitations | 220
- Open Issues | 222
- Resolved Issues | 223
- Documentation Updates | 229

Upgrading Using ISSU

In-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic.

For additional information about using ISSU on routing and switching devices, see the High Availability User Guide.

For additional information about using ISSU on security devices, see the Chassis Cluster User Guide for SRX Series Devices.

For information about ISSU support across platforms and Junos OS releases, see the In-Service Software Upgrade (ISSU) Web application.

Licensing

Starting in 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 have been developed at Juniper Networks over the past several years.

The major components of the framework are:

- A focus on customer segments (enterprise, service provider, and cloud) and use cases for Juniper Networks hardware and software products.
- The introduction of a common three-tiered model (standard, advanced, and premium) for all Juniper Networks software products.
- The introduction of subscription licenses and subscription portability for all Juniper Networks products, including Junos OS and Contrail.

For information about the list of supported products, see Juniper Flex Program.

Compliance Advisor

For regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6 for Juniper Networks products, see the Juniper Networks Compliance Advisor.

Finding More Information

- **Feature Explorer**—Juniper Networks Feature Explorer helps you in exploring 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. prsearch.juniper.net.
- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms. apps.juniper.net/hct/home

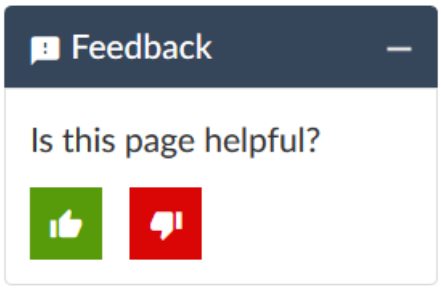
> **NOTE:** To obtain information about the components that are supported on the devices, and the special compatibility guidelines with the release, see the Hardware Guide for the product.

- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6 for Juniper Networks products. apps.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

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

Revision History

10 December 2021—Revision 11, Junos OS Release 20.1R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

7 October 2021—Revision 10, Junos OS Release 20.1R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

22 April 2021—Revision 9, Junos OS Release 20.1R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

13 January 2021—Revision 8, Junos OS Release 20.1R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

3 July 2020—Revision 7, Junos OS Release 20.1R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

25 June 2020—Revision 6, Junos OS Release 20.1R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

8 June 2020—Revision 5, Junos OS Release 20.1R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

7 May 2020—Revision 4, Junos OS Release 20.1R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

16 April 2020—Revision 3, Junos OS Release 20.1R1– PTX10003, PTX10008 Routers and the QFX5220 Switch.

3 April 2020—Revision 2, Junos OS Release 20.1R1– ACX Series, EX Series, MX Series, NFX Series,PTX Series, QFX Series, SRX Series, and Junos Fusion.

27 March 2020—Revision 1, Junos OS Release 20.1R1– ACX Series, EX Series, MX Series, NFX Series,PTX Series, QFX Series, SRX Series, and Junos Fusion.