Release Notes

Published
2021-08-26

Junos ® OS 18.2R1 Release Notes

SUPPORTED ON

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

HARDWARE HIGHLIGHTS

- Support for new universal metro routers (ACX5448)
- Support for xDSL SFP module (NFX Series)
- Support for QFX10000-30C-M line card channelization (QFX10008, QFX10016)

SOFTWARE HIGHLIGHTS

- Support for VPWS with EVPN signaling mechanisms and flexible cross connect (ACX5448)
- Support for virtualization (ACX5448)
- Support for 48x1/10GE and 4x100GE interface ports (ACX5448)
- Support for Layer 2 features (ACX5448)
- Support for Layer 3 features (ACX5448)
- Support for NSR and ISSU for point-to-multipoint LSP for EVPN provider tunnel (EX9200)
- Support for excluding the overhead bytes from queue statistics (MX Series)
- Support for OSPF, IS-IS, BGP, and static routing on IRB interfaces in EVPN-VXLAN networks (MX Series, vMX)
- Support for unified ISSU (MX10003)
- Support for PTP over Ethernet and hybrid mode over link aggregation group (MX Series)

- Support for ON_CHANGE expansion for Junos Telemetry Interface (JTI) (MX Series)
- Support for local authentication and authorization for subscribers (MX Series)
- Support for DHCP short-cycle protection to reduce excess loading (MX Series)
- Support for global range setting for initial router advertisement intervals (MX Series)
- Support for security features (NFX Series)
- Support for vMX VNF (NFX250-S1, NFX250-S2)
- Support for J-Insight device monitor (MX Series, vMX, and “PTX Series”)
- Support for client link-layer address option 79 for DHCPv6 (QFX Series)
- Support for zero touch provisioning (QFX10008, QFX10016)
- Support for advanced policy-based routing (APBR) policy (SRX Series, vSRX)
- Support for advanced features for logical systems (SRX Series, vSRX)
- Support for TWAMP ALG traffic (SRX Series)
- Support for unified policies (SRX Series, vSRX)

Release Notes: Junos® OS Release 18.2R1 for the ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion

26 August 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, and Junos Fusion.

These release notes accompany Junos OS Release 18.2R1 for the ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

NOTE: The recommended release for Junos Fusion Data Center is 18.1R2-S2. The subsequent 18.xRx mainline releases (18.2, 18.3, and 18.4) do not support Junos Fusion Data Center.

Junos OS Release Notes for ACX Series

IN THIS SECTION

These release notes accompany Junos OS Release 18.2R1 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

This section describes the features and enhancements in Junos OS Release 18.2R1 for ACX Series Universal Metro Routers.

Hardware

- **New ACX5448 Universal Metro Routers**—Starting with Junos OS Release 18.2R1, the ACX5448 Universal Metro Routers are available as Juniper Networks' top-of-rack router solutions for data centers and campus distribution or aggregation environments. The ACX5448 router portfolio consists of high-performance fixed-configuration routers that add higher port densities, additional scalability, and improved latency to the ACX Series. The ACX5448 routers offers a compact 1U model that provides wire-speed packet performance, very low latency, and a rich set of Layer 2 and Layer 3 features. The router has a high-throughput Packet Forwarding Engine, and the performance of the control-plane running on ACX5448 router is enhanced by the 1.9 Ghz six-core Intel CPU with 32 GB of memory and two 100 GB of solid-state drive (SSD) storage.

  The ACX5448 is a 10-Gigabit Ethernet enhanced small form-factor pluggable (SFP+) top-of-rack router with 48 SFP+ ports, and four 100-Gigabit Ethernet QSFP28 ports. Each SFP+ port can operate as a native 10-Gigabit Ethernet port, or as a 1-Gigabit Ethernet port when 1-Gigabit optics are inserted.

  The ACX5448 is shipped with redundant fans and redundant power supplies. The router can be ordered with front-to-back airflow (air out or AFO), or back-to-front airflow (air in or AFI), and with AC or DC power supplies.

Authentication Access Control

- **Enhancement to NTP authentication method (ACX500, ACX1100)**— Starting in Junos OS Release 18.2R1, Junos OS supports NTP authentication for both SHA-1 and SHA2-256, in addition to the existing NTP authentication method, MD5. You can now choose from among MD5, SHA-1, and SHA2-256 for synchronizing the clocks of Juniper Network routers, switches, and other security devices on the Internet. Using SHA-1 instead of MD5 improves the security of devices with very little impact to timing, while using SHA2-256 provides an increase in security over SHA-1.

  > **NOTE:** By default, network time synchronization is unauthenticated.

  To implement authentication, use **set authentication-key <*key_number*> type** at the **[edit system ntp]** hierarchy level.

  - To enable SHA-1 authentication, use **set authentication key <*key_number*> type sha1 value <*password*>** at the **[edit system ntp]** hierarchy level.
  - To enable SHA2-256 authentication, use **set authentication key <*key_number*> type sha256 value <*password*>** at the **[edit system ntp]** hierarchy level.

See authentication-key and Configuring NTP Authentication Keys

Class of Service

- **Support for logical interface-based classification and rewrites (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports configuring logical interface-based classification and rewrite rules. ACX5448 router supports fixed, behavior aggregate (IP precedence, DSCP, DSCP IPv6, MPLS EXP, IEEE-802.1p, IEEE-802.1ad (DEI bit)), and multifield classifiers.

  See Classifiers and Rewrite Rules at the Global, Physical and Logical Interface Levels Overview

- **Support for port-based queueing, scheduling, and shaping (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports port-based queueing, scheduling, and shaping. You can configure up to eight queues (virtual output queues) per physical interface (port). Scheduling properties can be applied at both physical as well as logical interface levels. The egress scheduler supports two priority levels (**strict-high** and **low**). Multiple strict-high priority queues and multiple low (default) priority queues can be configured.

  Schedulers and their associated shapers control the traffic bandwidth, jitter (delay variation), and packet loss priority at the egress of the device. By default a port on ACX5448 router gets a dedicated buffer of 100ms and shared buffer from DRAM. Delay buffer controls the latency of the queue during congestion and maximum number of packets that can be held in a queue. Default buffer size per port is 100ms.

  See Understanding Schedulers Overview, Configuring Shared and Dedicated Buffer Memory Pools, and Hierarchical Class of Service in ACX5000.

Dynamic Host Configuration Protocol

- **Support for DHCPv4 and DHCPv6 (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports DHCP server, DHCP client, and DHCP relay configuration for IPv4 and IPv6 services. You can enable ACX5448 router to function as DHCP server and configure the DHCP server options on the router. The DHCP server provides an IP address and other configuration information in response to a client request. DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

  See Extended DHCP Local Server Overview and See Extended DHCP Relay Agent Overview

EVPN

- **Support for VPWS with EVPN signaling mechanisms and flexible cross connect (ACX5448)**—Starting with Junos OS Release 18.2R1, the ACX5448 router supports VPWS with EVPN signaling mechanisms and flexible cross connect. The EVPN VPWS provides a framework for delivering the VPWS with EVPN signaling mechanisms. The VPWS with EVPN signaling mechanisms supports single-active or all-active multihoming capabilities and inter-autonomous system (AS) options associated with BGP-signaled VPNs.

The EVPN VPWS flexible cross connect addresses the label resource issue. The flexible cross-connect (FXC) service enables interoperability of access router that uses EVPN FXC VLAN-aware and VLAN-unaware FXC services. ACX5448 router do not support pseudowire services in EVPN VPWS flexible cross connect.

The following limitations apply:

- Control word is not supported for EVPN VPWS services.
- When VLAN maps are applied on the ccc-interfaces (UNI) for EVPN VPWS, only the following VLAN map operations are applicable:

```
IFD Encap/      IFL-TYPE         Input-MAP       Output-Map
-----------------------------------------------------------------
ethernet-ccc    unit 0;
                TC2             push-push       pop-pop

vlan-ccc
                ST: vlan-id X
                                swap-push        ..
                DT: vlan-tags outer  X  inner Y
                TC1             pop-pop         push-push
                TC4             swap-swap       swap-swap
```

- VLAN map with non-default TPIDs in the VLAN map operation is not supported.
- Aggregated Ethernet interfaces with LAG interface for EVPN VPWS and EVPN VPWS FXC services are not supported. However, for CE multihoming, the CE can have static-AE, and CE can multihome to the ACX5448 PE router (PE in non-AE/LAG).

See Overview of VPWS with EVPN Signaling Mechanisms

General Routing

- **Support for virtualization (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 routers support virtualization. Virtualization enables multiple instances of operating systems, called guests, to run concurrently on the host and share virtualized hardware resources. A guest is a virtual machine (VM) that runs on a hypervisor-based host and shares its resources. A host is a virtualized software whose hypervisor allows multiple guest VMs to run on it concurrently and share its resources. A VM can be an instance of Junos OS or any compatible third-party VM. Each VM runs its own operating system image and applications that can be different from that of another VM running on the same host. ACX5448 router supports only one Junos VM. You can use the following chassis management commands to manage the onboard FRUs:

- **show chassis hardware**
- **show chassis temperature-thresholds**
- **show chassis environment**
- **show chassis alarms**

ACX5448 router emulates one FPC with two PICs. One PIC represents the 48x1/10GE ports and other represents the 4x100GE ports. The **show chassis hardware** CLI command shows the FPC and PICs as built-in as shown in the following sample output:

user@host> **show chassis hardware**

```
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                DA805             ACX5448
Midplane         REV 13   750-065110   ACNP4346          ACX5448
Routing Engine            BUILTIN      BUILTIN           Routing Engine
RFEB
FPC 0                     BUILTIN      BUILTIN           FPC BUILTIN
  MIC 0                                                  48x1GE/48x10GE
    PIC 0                 BUILTIN      BUILTIN           48x1GE/48x10GE
  MIC 1                                                  24x10/25GE 6x40/100GE
    PIC 1                 BUILTIN      BUILTIN           24x10/25GE 6x40/100GE
```

NOTE: ACX5448 routers do not support **request system software upgrade** and **request system software rollback** commands, instead you must use **request vmhost** CLI commands.

ACX5448 routers do not support:

- Multiple guest VMs
- Redundant Junos VMs
- ISSU
- 10/100 Mbps copper SFPs

See Routing Engines with VM Host Support and Architecture of Routing Engines with VM Host Support

Routing Policy and Firewall Filters

- **Support for firewall filters and policers (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports configuring firewall filters on packets (families such as bridge domain, IPv4, IPv6, CCC, MPLS) based on packet match conditions. Along with the match conditions, actions such as count, discard, log, syslog, policer are performed on the packets that match the filter. You can configure policers and attach them to a firewall term.

  See Standard Firewall Filter Match Conditions and Actions on ACX Series Routers Overview

Interfaces and Chassis

- **Support for 48x1/10GE and 4x100GE Interface Ports (ACX5448)**—ACX5448 router has 48x1/10GE interface ports and 4x100GE interface ports. The 48 ports on ACX5448 router can be configured as 1GE or 10GE modes and these ports are represented by **xe** interface type. The PIC 1 of FPC 0 has 4x100GE ports, where each port can be channelized as 1x100GE, or 1x40GE, or 4x25GE modes and these ports are represented by **et** interface type. By default, the port speed in PIC 1 is 100GE.

  See Understanding Interfaces on ACX Series Universal Metro Routers

Layer 2 Features

- **Support for Layer 2 features (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports the Layer 2 bridging, Q-in-Q tunneling, no-local switching, and Layer 2 protocol tunnel. A bridge domain is a set of logical interfaces that share the same flooding or broadcast characteristics. Layer 2 logical interfaces are created by defining one or more logical units on a physical interface with encapsulation as **vlan-bridge** and as **ethernet-bridge**. All the member ports of the bridge domain participate in Layer 2 learning and forwarding. These bridging features are used to configure E-LINE, E-LAN and E-TREE services. On ACX5448 router, you can configure bridge domains by using the following methods:

  - Bridge domain without a vlan-id number statement
  - Bridge domain with the vlan-id value set to none
  - Bridge domain with a single vlan-id

  The Layer 2 Next Generation mode, also called Enhanced Layer 2 Software (ELS), is supported on ACX5448 router for configuring the Layer 2 features.

  If **no-local-switching** is configured in a bridge domain, then traffic cannot flow between CE to CE interfaces. This includes known unicast/multicast, unknown unicast/multicast, and broadcast traffic. However, traffic can flow between CE to PE interfaces and between PE to PE interfaces.

  Q-in-Q tunneling allows you to create a Layer 2 Ethernet connection between two customer sites. Providers can segregate different customers' VLAN traffic on a link (for example, if the customers use overlapping VLAN IDs) or bundle different customer VLANs into a single service VLAN. Service providers

can use Q-in-Q tunneling to isolate customer traffic within a single site or to enable customer traffic flows across geographic locations.

Layer 2 protocol tunnel can be configured on the customer edge port using mac rewrite configuration. MAC rewrite is supported for the STP, CDP, VTP, LLDP, ELMI, 802.1x, 802.3ah, LACP, MMRP, MVRP protocol packets.

See Layer 2 Bridge Domains on ACX Series Overview, See Q-in-Q Tunneling on ACX Series Overview, and See Understanding Layer 2 Next Generation Mode on ACX Series Routers

- **Support for Layer 2 services (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports configuring Layer 2 services such as RSTP, MSTP for loop resolutions, and storm control to monitor traffic levels and to drop broadcast, unknown unicast, and multicast (BUM) packets if they exceed the configured limit.

  Storm control is applied on the following traffic types:

  - Layer 2 multicast packets
  - Layer 2 unregistered multicast packets
  - Layer 2 registered multicast packets

  On ACX5448 router, storm control is only applicable at the physical interface level. No event will be logged when a traffic storm hits an ACX5448 router. Also interfaces will not be bound to any default profile. The default action is to drop the packets exceeding the configured bandwidth.

  See Storm Control on ACX Series Routers Overview

- **Support for Layer 2 protection (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports configuring bridge protocol data unit (BPDU) protect, loop protect, and root protect on spanning-tree instance interface. You can configure BPDU protection on individual interfaces or on all the edge ports of the bridge.

  See Understanding BPDU Protection for Spanning-Tree Instance Interfaces, Understanding Loop Protection for Spanning-Tree Instance Interfaces, and Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network

Layer 3 Features

- **Support for Layer 3 features (ACX5448)**—Starting with Junos OS Release 18.2R1, the ACX5448 router uses MPLS as a transport mechanism and they include support for label-switching router (LSR), label edge routers (LERs), and pseudowire services. The protocols such as ECMP, OSPF, ISIS, and BGP are also supported on ACX5448 router.

  See MPLS Overview

Management

- **Support for NETCONF over SSH and custom YANG models (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports NETCONF OVER SSH and custom YANG modules.

  Client applications can access the NETCONF server using the SSH protocol and use the standard SSH authentication mechanism. After authentication, the NETCONF server uses the configured Junos OS login usernames and classes to determine whether a client application is authorized to make each request.

  You can load custom YANG modules on the router to add data models that are not natively supported by Junos OS but can be supported by translation. Doing this enables you to extend the configuration hierarchies and operational commands with data models that are customized for your operations. You can load custom YANG modules by using the **request system yang add** operational command.

  See Establishing an SSH Connection for a NETCONF Session and YANG Modules Overview

MPLS

- **Support for MPLS ping and Bidirectional Forwarding Detection over virtual circuit connection verification (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports MPLS ping and Bidirectional Forwarding Detection over Virtual Circuit Connection Verification. MPLS ping functionality diagnoses the state of label-switched paths (LSPs), where the router sends probe packets into the LSP. Based on how the LSP at the remote endpoint of the connection replies to the probes, you can determine the connectivity of the LSP. Each probe is an echo request sent to the LSP as an MPLS packet with a UDP payload. If the outbound node receives the echo request, it checks the contents of the probe and returns a value in the UDP payload of the response packet. If the Junos OS receives the response packet, it reports a successful ping response.

  Bidirectional Forwarding Detection (BFD) support for virtual circuit connection verification (VCCV) allows you to configure a control channel for a pseudowire, in addition to the corresponding operations and management functions to be used over that control channel. BFD provides a low resource mechanism for the continuous monitoring of the pseudowire data path and for detecting data plane failures, as described in RFC 5885.

  You can use the following commands for debugging:

  - show bfd session extensive

- show ldp database extensive

See Pinging LSPs and Configuring BFD for VCCV for Layer 2 Circuits

- **Support for MPLS ping and traceroute (ACX5448)**—Starting with Junos OS Release 18.2R1, the ACX5448 router supports MPLS ping and traceroute. MPLS ping and traceroute [RFC-4379] are common tools used to debug connectivity between two PEs for a LSP. The ping portion works by injecting an echo request packet in a LSP and expecting the remote PE endpoint to receive and reply to the packet. The traceroute function works the same as it does for IP where it sends multiple packets with an increasing TTL to let the packet get progressively farther in the LSP path before sending message indication that the TTL has expired.

  See Pinging LSPs

Multicast

- **Support for multicast features (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports the following multicast protocol (IGMP and PIM) features for forwarding IPv4 and IPv6 traffic:
  - Anycast rendezvous point
  - Auto rendezvous point
  - Bidirectional Forwarding Detection (BFD) for PIM
  - IGMP version 1, version 2, and version 3
  - IGMP filter
  - IGMP proxy (relay)
  - IGMP querier
  - IGMP version 1, version 2, and version 3 snooping
  - Multicast Source Discovery Protocol (MSDP)
  - PIM static rendezvous point
  - PIM source-specific multicast (SSM)
  - PIM sparse mode

See Multicast Overview

Routing Protocols

- **Support for Two-Way Active Measurement Protocol (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports Two-Way Active Measurement Protocol (TWAMP). The TWAMP defines a standard for measuring IP performance between two devices in a network. ACX5448 router supports only the reflector side of TWAMP.

  See Understanding Two-Way Active Measurement Protocol on Routers

Security

- **Support for secure boot and BIOS (ACX5448)**—Starting with Junos OS Release 18.2R1, a significant system security enhancement, secureboot, has been introduced in ACX5448 router. The secureboot implementation is based on the UEFI 2.4 standard. BIOS in ACX5448 router has been hardened and is responsible for initializing all the components of the router hardware. The following are some of the key functionalities supported by the BIOS in ACX5448 router:
  - Initialization of hardware components
  - Watchdog support
  - Booting the operating system
  - Diagnostics support
  - Secure boot support

  See Feature Explorer and enter Secure Boot.

Software Installation and Upgrade

- **Firmware upgrade (ACX6360 Router)**—Starting in Junos OS Release 18.2R1, you can install or upgrade the system firmware on ACX6360 router.

  Install the firmware package by using:

  - **request system firmware add *path/package-name***

  Upgrade an existing firmware, by using any of the following command:

  - **request system firmware upgrade pic**
  - **request system firmware upgrade cb**
  - **request system firmware upgrade re**
  - **request system firmware upgrade fpc**

On the ACX6360 line card, you upgrade the following firmware components:

- Uboot—Responsible for loading the operating system on the line card
- FPGA—Controls all functions of the line card

You can also upgrade the following firmware components:

- RE- FPGA—The RE-FPGA is located on the control board and manages board initialization, reboot, and other functions.
- TIC-FPGA—The TIC-FPGA is located on the 8x CFP2 optical port card and manages access to the optical functions.
- FTC FPGA—The FTC FPGA is located on the fan controllers and controls the fan controllers.
- FPD FPGA—The FPD FPGA is located on the LED board and is responsible for the LED board.
- SIB FPGA—The SIB FPGA is located on the SIB and handles the SIBs

Timing and Synchronization

- **Support for PTP transparent clock (ACX5448)**—Starting with Junos OS Release 18.2R1, ACX5448 router supports the PTP transparent clock functionality for PTP over IP, as well as PTP over Ethernet. A certain amount of delay is always experienced by the PTP packets due to queuing and buffering within the router, which could be due to network load or based on the architecture of the router. The PTP transparent clock measures the residence time (the time that the packet spends passing through the router), and adds the residence time into the correction field of the PTP packet. ACX5448 routers support end-to-end transparent clocks. With an end-to-end transparent clock, only the residence time is included in the correction field of the PTP packets. ACX5448 supports end-to-end (e2e) transparent clocks as defined in IEEE1588.

  See Understanding Transparent Clocks in Precision Time Protocol

SEE ALSO

Changes in Behavior and Syntax | 25

Known Behavior | 26

Known Issues | 26

Resolved Issues | 28

Documentation Updates | 29

Migration, Upgrade, and Downgrade Instructions | 29

Product Compatibility | 30

Changes in Behavior and Syntax

IN THIS SECTION

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 18.2R1 for the ACX Series routers.

High Availability (HA) and Resiliency

- **commit fast-synchronize** option not supported for products with single Routing Engine (ACX Series)—Starting in Junos OS Release 18.2R1, Junos OS does not support the configuration option **commit fast-synchronize** at the **[edit system]** hierarchy level for all the products with single Routing Engine for which **chassis redundancy graceful-switchover** is not supported. This option is disabled from the CLI.

Junos XML API and Scripting

- **Junos XML protocol <open-configuration> operation no longer emits an uncommitted changes warning (ACX Series)**—Starting in Junos OS Release 18.2R1, the Junos XML protocol **<open-configuration>** operation does not emit an "**uncommitted changes will be discarded on exit**" warning message when opening a private copy of the candidate configuration. However, Junos OS still discards the uncommitted changes upon closing the private copy.

Layer 3 Features

- **DMA recovery mechanism (ACX Series)**—Starting in Junos OS Release 18.2R1, a potential recovery mechanism has been introduced that is triggered in case the router enters an **Idle** state on any DMA channels. The recovery mechanism resets the necessary registers to recover from failure conditions and therefore a PFE reboot is not required. The following recovery success message is logged in the PFE syslog message:

```
BCM DMA error recovery: Recovery complete Success
```

SEE ALSO

Known Behavior

There are no known limitations in Junos OS Release 18.2R1 for the ACX Series.

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

SEE ALSO

Known Issues

IN THIS SECTION

This section lists the known issues in hardware and software in Junos OS Release 18.2R1 for the ACX Series Universal Metro Routers.

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

Class of Service

- On ACX5448 router, when loss priority is configured as either **medium-low** or **medium-high**, the rewrite rule gets applied for loss priority **low**. PR1358721
- On ACX5448 router, the **clear interfaces statistics all** CLI command takes long time to respond with scaled interfaces configured. PR1366087

DHCP

- On ACX5448 router, when an ingress interface is configured as a LAG interface and if DHCP request packets arrive at that LAG Interface, the router might drop the packets erroneously. PR1353887
- On ACX5448 router, when an ingress interface is configured as a XE Interface and if DHCP request packets arrive at that XE interface, the router might drop the packets erroneously. PR1347906

IGMP Snooping

- The IGMP snooping feature does not work on the ACX5448 router. PR1351422

Timing and Synchronization

- When an ACX5448 router is configured as PTP-TC, incorrect UDP checksum errors are seen when checksum 0x0 is sent from the transmitting node. This occurs when a packet type of 1588 enters the ACX5448 router with UDP.checksum == 0x0 and the checksum field gets partially updated and the packet egresses the router with an incorrect checksum. This incorrect checksum causes packet drops in the next device. PR1327155

SEE ALSO

- New and Changed Features | 14
- Changes in Behavior and Syntax | 25
- Known Behavior | 26
- Resolved Issues | 28
- Documentation Updates | 29
- Migration, Upgrade, and Downgrade Instructions | 29
- Product Compatibility | 30

Resolved Issues

There are no fixed issues in Junos OS 18.2R1 for ACX Series.

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

SEE ALSO

- New and Changed Features | 14
- Changes in Behavior and Syntax | 25
- Known Behavior | 26
- Known Issues | 26

Documentation Updates

There are no errata or changes in Junos OS Release 18.2R1 for the ACX Series documentation.

SEE ALSO

New and Changed Features | 14
Changes in Behavior and Syntax | 25
Known Behavior | 26
Known Issues | 26
Resolved Issues | 28
Migration, Upgrade, and Downgrade Instructions | 29
Product Compatibility | 30

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

- New and Changed Features | 14
- Changes in Behavior and Syntax | 25
- Known Behavior | 26
- Known Issues | 26
- Resolved Issues | 28
- Documentation Updates | 29
- Product Compatibility | 30

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 31

Hardware Compatibility

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

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

Hardware Compatibility Tool

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

SEE ALSO

New and Changed Features | **14**

Changes in Behavior and Syntax | **25**

Known Behavior | **26**

Known Issues | **26**

Resolved Issues | **28**

Documentation Updates | **29**

Migration, Upgrade, and Downgrade Instructions

Junos OS Release Notes for EX Series Switches

IN THIS SECTION

These release notes accompany Junos OS Release 18.2R1 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

This section describes the new features and enhancements to existing features in Junos OS Release 18.2R1 for the EX Series.

> **NOTE:** The following EX Series switches are supported in Release 18.2R1: EX2300, EX3400, EX4300, EX4600, and EX9200.

Hardware

- **EX4300-48MP and EX4300-48MP-S switches**—Starting with Junos OS Release 18.2R1, two new models of EX4300 switches are available—EX4300-48MP and EX4300-48MP-S switches. These models provide 24 built-in 10/100/1000BASE-T Ethernet network ports, 24 built-in 100/1000/2500/5000/10000BASE-T Ethernet network ports, and four built-in 40-Gigabit Ethernet quad small form-factor pluggable plus (QSFP+) ports that can house 40-Gigabit QSFP+ transceivers. The 24 built-in 10/100/1000BASE-T Ethernet network ports support 10 Mbps, 100 Mbps, and 1 Gbps speeds. The 24 built-in 100/1000/2500/5000/10000BASE-T Ethernet network ports support 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps speeds. All network ports are equipped for PoE+ and provide up to 95 watts of power. The QSFP+ ports are configured as Virtual Chassis Ports (VCPs) by default. You can use them to connect the switches to other devices in a Virtual Chassis configuration.

  [See EX4300 Switch Hardware Guide.]

- **EX9253 switches**—Starting with Junos OS Release 18.2R1, EX9253 switches are available as a modular switch. The switch has two dedicated slots for line cards and supports EX9253-6Q12C and EX9253-6Q12C-M line cards. The switch is available in two variants—with AC power supply and with DC power supply.

  [See EX9253 Switch Hardware Guide.]

Authentication, Access Control

- **Enhancement to NTP authentication method (EX4300)**— Starting in Junos OS Release 18.2R1, Junos OS supports NTP authentication for both SHA-1 and SHA2-256, in addition to the existing NTP authentication method, MD5. You can now choose from among MD5, SHA-1, and SHA2-256 for synchronizing the clocks of Juniper Network routers, switches, and other security devices on the Internet. Using SHA-1 instead of MD5 improves the security of devices with very little impact to timing, while using SHA2-256 provides an increase in security over SHA-1.

  > **NOTE:** By default, network time synchronization is unauthenticated.

  To implement authentication, use **set authentication-key *<key_number>* type** at the **[edit system ntp]** hierarchy level.

  - To enable SHA-1 authentication, use **set authentication key *<key_number>* type sha1 value *<password>*** at the **[edit system ntp]** hierarchy level.
  - To enable SHA2-256 authentication, use **set authentication key *<key_number>* type sha256 value *<password>*** at the **[edit system ntp]** hierarchy level.

See authentication-key and Configuring NTP Authentication Keys

Authentication, Authorization, and Accounting (AAA)

- **RADIUS over IPv6 (EX Series)**—Starting with Junos OS Release 18.2R1, EX2300, EX3400, EX4600 and EX4300-48MP switches support IPv6 for user authentication, authorization, and accounting (AAA) using RADIUS servers, in addition to the existing IPv4 support. You can specify which source address Junos OS uses to contact an external RADIUS server. To configure an IPv6 source address for RADIUS authentication, include the **source-address** statement at the [**edit system radius-server *server-address***] hierarchy level. To configure an IPv6 source address for RADIUS accounting, include the **source-address** statement at the [**edit system accounting destination radius server *server-address***] hierarchy level.

  [See source-address.]

Class of Service (CoS)

- **Support for setting unique IEEE 802.1p code point for host-generated RPM packets (EX2300, EX3400, EX4300)**—You can already set the DSCP code point and IEEE 802.1p code point for all host-generated packets by setting the **dscp-code-point *code-point-value*** option at the **[class-of-service host-outbound-traffic]** hierarchy level, where the first three bits of the defined DSCP code point value are set as the IEEE 802.1p code point value. Starting with Junos OS 18.2R1, you can override this IEEE 802.1p code point value for host-generated RPM packets and set a separate value for these packets by setting the **dscp-code-point *code-point-value*** option at the **[services rpm probe *owner* test *test-name*]** hierarchy level, where again the first three bits of the defined DSCP code point value are set as the IEEE 802.1p code point value.

  [See dscp-code-point (Services).]

Dynamic Host Configuration Protocol (DHCP)

- **DHCP smart relay (EX4600)**—Starting with Junos OS Release 18.2R1, you can configure alternative IP addresses for the gateway interface so that if the server fails to reply to the requests sent from the primary gateway address, the switch can resend the requests using alternative gateway addresses. To use this feature, you must configure an IRB interface or Layer 3 subinterface with multiple IP addresses and configure that interface as a relay agent.

  [See Configuring DHCP and BOOTP Relay.]

EVPN

- **NOTE:** NSR and unified ISSU support for point-to-multipoint LSP for EVPN provider tunnel is documented but not supported in Junos OS Release 18.2R1.

  NSR and unified ISSU support for point-to-multipoint LSP for EVPN provider tunnel (EX9200)—Starting in Junos OS Release 18.2R1, Junos OS provides nonstop routing (NSR) and unified ISSU support for point-to-multipoint (P2MP) inclusive provider tunnels. This ensures that broadcast, unknown unicast, and multicast (BUM) packets continue after a Routing Engine switchover occurs when NSR is enabled.

  [See *Understanding P2MPs LSP for the EVPN Inclusive Provider Tunnel*.]

- **IGMP snooping support for EVPN-MPLS (EX9200)**—Starting with Junos OS Release 18.2R1, you can configure IGMP snooping on EX9200 switches in an Ethernet VPN (EVPN) over an MPLS network. Enabling IGMP snooping helps to constrain multicast traffic to interested receivers in a broadcast domain.

  Multicast sources and receivers in the EVPN instance (EVI) can each be single-homed to one provider edge (PE) device or multihomed (in all-active mode only) to multiple PE devices. When IGMP snooping is configured with multihomed receivers, IGMP state information is synchronized among peer PE devices by exchanging BGP EVPN Type 7 (Join Sync Route) and Type 8 (Leave Sync Route) network layer reachability information (NLRI). When PE devices receive multicast traffic from the EVPN core on a multihomed Ethernet segment (ES), only the designated forwarder (DF) PE device forwards the traffic, and the DF forwards the traffic only to interested receivers (selective multicast forwarding) based on IGMP snooping reports and BGP EVPN Type 7 routes. PE devices serving single-homed receivers also use selective multicast forwarding based on IGMP snooping reports to forward the traffic only to interested receivers, conserving network bandwidth.

  All PE devices perform inclusive multicast forwarding using ingress replication to forward multicast traffic into the EVPN core to reach all remote PE devices. Multicast traffic at Layer 3 is routed between bridge domains or VLANs using IRB interfaces.

  This feature is supported with multiple EVIs, multicast sources and receivers on the same or different sites, and IGMP snooping in proxy mode only.

  To enable IGMP snooping on PE devices in an EVPN instance, include the **igmp-snooping proxy** statement at the [**edit routing-instances *routing-instance-name* protocols**] or the [**edit routing-instances *routing-instance-name* bridge-domain *bridge-domain-name* protocols**] hierarchy level.

  For inter-VLAN multicast forwarding, PIM distributed DR (PIM DDR) mode must be enabled on all participating IRBs.

  EVPN and IGMP snooping operational mode commands can be used to view information learned from IGMP snooping messages or EVPN Type 7 and Type 8 messages.

  [See Overview of Multicast Forwarding with IGMP Snooping in an EVPN-MPLS Environment.]

- **Support for OSPF, IS-IS, BGP, and static routing on IRB interfaces in EVPN-VXLAN networks (EX Series)**—Starting in Junos OS Release 18.2R1, you can configure OSPF, IS-IS, BGP, and static routing with Bidirectional Forwarding Detection (BFD) on an IRB interface that is used as a routed interface in

EVPN. This allows protocol adjacencies to be established between an IRB on a Layer 3 gateway and a CE device and between an IRB on a Layer 3 gateway and a CE device connected to a Layer 2 leaf device in an EVPN-VXLAN network.

[See Supported Protocols on an IRB Interface in EVPN-VXLAN .]

- **NOTE:** This feature is documented but not supported in Junos OS Release 18.2R1

EVPN P2MP bud node support (EX9200)—Starting in Junos OS Release 18.2R1, Junos OS supports configuring a point-to-multipoint (P2MP) label-switched path (LSP) as a provider tunnel on a bud node. The bud node functions both as an egress node and a transit node.

To enable a bud node to support P2MP LSP, include the **evpn p2mp-bud-support** statement at the **[edit routing-instances routing-instance-name protocols evpn]** hierarchy level.

[See Configuring Bud Node Support.]

- **Layer 2 VXLAN gateway in EVPN-VXLAN overlay network (EX4600 switches)**—By using a Layer 3 IP-based underlay network coupled with an Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) overlay network, you can deploy larger networks than those possible with traditional Layer 2 Ethernet-based architectures. With overlay networks, endpoints (bare-metal servers [BMSs] or virtual machines [VMs]) can be placed anywhere in the network and remain connected to the same logical Layer 2 network, enabling the virtual topology to be decoupled from the physical topology.

  The physical underlay network over which EVPN-VXLAN is commonly deployed is a two-layer IP fabric, which includes spine and leaf devices. The spine devices provide connectivity between the leaf devices, and the leaf devices function as Layer 2 VXLAN gateways and provide connectivity to the attached endpoints. Starting with Junos OS Release 18.2R1, you can deploy EX4600 switches as leaf nodes in the EVPN-VXLAN overlay network.

  [See Understanding EVPN with VXLAN Data Encapsulation.]

- **EVPN-VXLAN support of Virtual Chassis (EX4600, EX4600 Virtual Chassis)**—Ethernet VPN (EVPN) supports multihoming active-active mode, which enables a host to be connected to two leaf devices through a Layer 2 LAG interface. Starting with Junos OS Release 18.2R1, the two leaf devices can be EX4600 standalone switches or EX4600 switches configured as a Virtual Chassis.

  On each leaf device, the LAG interface is configured with the same Ethernet segment identifier (ESI) for the host. The two leaf devices on which the same ESI is configured are peers to each other.

[See EVPN-VXLAN Support of Virtual Chassis and Virtual Chassis Fabric.]

- **Tunneling Q-in-Q traffic through an EVPN-VXLAN overlay network (EX4600 switches)**—Starting in Junos OS Release 18.2R1, EX4600 switches that function as Layer 2 VXLAN tunnel endpoints (VTEPs) can tunnel single-tagged and double-tagged Q-in-Q packets through an Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) overlay network. In addition to tunneling Q-in-Q packets, the ingress and egress VTEPs can perform the following Q-in-Q actions:

  - Delete, or pop, an outer service VLAN (S-VLAN) tag from an incoming packet.
  - Add, or push, an outer S-VLAN tag onto an outgoing packet.
  - Map a configured range of customer VLAN (C-VLAN) IDs to an S-VLAN.

  > **NOTE:** EX4600 switches do not support the pop and push actions with a configured range of VLANs.

  The ingress and egress VTEPs support the tunneling of Q-in-Q packets and the Q-in-Q actions in the context of specific traffic patterns.

  [See Examples: Tunneling Q-in-Q Traffic in an EVPN-VXLAN Overlay Network.]

Interfaces and Chassis

- **Support for hyper mode to increase packet processing rate on line cards with enhanced MPCs (EX9200 switches)**—Starting in Junos OS Release 18.2R1, EX9200 line cards that include enhanced MPCs (such as MPC4E and MPC5E) support the hyper mode feature. Enabling the hyper mode feature increases the rate at which a data packet is processed, which results in the optimization of the lifetime of a data packet. Optimization of the data packet lifetime enables better performance and throughput.

  > **NOTE:** You can enable hyper mode only if the network-service mode on the switch is configured as either **enhanced-ip** or **enhanced-ethernet**. Also, you cannot enable the hyper mode feature for a specific Packet Forwarding Engine on an MPC—that is, when you enable the feature, it is applicable for all Packet Forwarding Engines on the switch.

  When you enable the hyper mode feature, the following actions and features are not supported:

  - Creating Virtual Chassis.
  - Padding Ethernet frames with VLANs.
  - Sending Internet Control Message Protocol (ICMP) redirect messages.
  - Terminating or tunneling subscriber-based services.

[See Understanding the Hyper Mode Feature on Enhanced MPCs for MX Series Routers and EX9200 Switches.]

- **Multi-rate and non-multi rate support (EX4300-MP Switches)**—Starting in Junos OS Release 18.2R1, you configure an interface to now support multiple speeds on EX4300-MP switches. The interfaces now support 2.5G, 5G, and 10G speeds. The interfaces earlier supported only 100M and 1G speeds.

  The naming convention for multi-rate interfaces (including 100M and 1G) is “mge-n/n/n”. The differentiation between multi-rate interfaces and 1G interfaces is based on the speed values. The front panel ports have different color coding to differentiate multi-rate and 1G interfaces.

- **4x10SFP+ Uplink Modules support (EX4300-MP Switches)**—Starting in Junos OS Release 18.2R1, you can configure the operating mode on the module to match the type of transceiver you want to use. EX4300-MP switches contain four ports for 10-gigabit small form-factor pluggable (SFP+) transceivers when configured to operate in 10-gigabit mode.

Layer 2 Features

- **L2PT support for tunneling additional protocols (EX2300 and EX3400 switches)**—Starting with Junos OS Release 18.2R1, you can configure Layer 2 protocol tunneling (L2PT) for the following new protocols on EX2300 and EX3400 switches: E-LMI, IEEE 802.1X, MMRP, and UDLD.

  > **NOTE:** Support for tunneling these additional protocols does not apply to multigigabit models of the EX2300 switch (EX2300-24MP or EX2300-48MP).

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

- **Ethernet ring protection switching (ERPS)(EX2300 and EX3400 switches and Virtual Chassis)**—Starting in Junos OS Release 18.2R1, you can use ERPS to reliably achieve carrier-class network requirements for Ethernet topologies forming a closed loop. ITU-TRecommendation G.8032 version 1 is supported.

  ERPS version 1 comprises the following features:

  - Support for revertive mode of operation of the Ethernet ring
  - Support for multiple ring instances on the same interfaces
  - Support for multiple ring instances on different interfaces
  - Support for interworking with Spanning Tree Protocol, Multiple Spanning Tree Protocol, and redundant trunk groups

  [See Understanding Ethernet Ring Protection Switching Functionality.]

Operation, Administration, and Maintenance (OAM)

- **Ethernet Connectivity Fault Management (CFM) Support (EX2300 and EX3400 Switches)**—Starting with Junos OS Release 18.2R1, Connectivity Fault Management (CFM) is supported on EX2300 and EX3400 switches. The major features of CFM are:
  - Fault monitoring using the continuity check protocol. This is a neighbor discovery and health check protocol that discovers and maintains adjacencies at the VLAN or link level.
  - Path discovery and fault verification using the linktrace protocol. Similar to IP traceroute, this protocol maps the path taken to a destination MAC address through one or more bridged networks between the source and destination
  - Fault isolation using the loopback protocol. Similar to IP ping, this protocol works with the continuity check protocol during troubleshooting.

  You can configure the Ethernet CFM using the **set protocols oam ethernet connectivity-fault-management** command, and verify the configuration using the **show oam ethernet connectivity-fault-management** command.
- **Ethernet link fault management (LFM) support (EX4600 switches)**—Starting with Junos OS Release 18.2R1, link fault management (LFM) is supported on EX4600 switches. Ethernet OAM provides the tools that network management software and network managers can use to determine how a network of Ethernet links is functioning. The following OAM LFM features are supported:
  - Discovery and link monitoring
  - Remote fault detection

Port Security

- **Media Access Control security with 256-bit cipher suite (EX9200)—**Starting in Junos OS Release 18.2R1, the GCM-AES-256 cipher suite for MACsec in static CAK mode is supported on EX9200 switches with EX9200-40XS line cards installed. The GCM-AES-256 cipher suite has a maximum key length of 256 bits and is also available with extended packet numbering (GCM-AES-XPN-256).

  [See Understanding Media Access Control Security (MACsec).]
- **IP source guard (EX2300 and EX3400 switches and Virtual Chassis)**—Starting with Junos OS Release 18.2R1, you can configure the IP source guard access port security feature to mitigate the effects of source IP address spoofing and source MAC address spoofing. If IP source guard determines that a host connected to an access interface has sent a packet with an invalid source IP address or source MAC address in the packet header, it discards the packet.

  [See Understanding IP Source Guard for Port Security on EX Series Switches.]

- **Support for 802.1X authentication on private VLANs (PVLANs) (EX2300, EX3400, and EX4300 switches and Virtual Chassis)**—Starting in Junos OS Release 18.2R1, you can enable 802.1X (dot1x) authentication for security purposes on access ports that are in a PVLAN.

  PVLANs provide Layer 2 isolation between ports within a VLAN, splitting a broadcast domain into multiple discrete broadcast subdomains by creating secondary VLANs. PVLANs are useful for restricting the flow of broadcast and unknown unicast traffic and for limiting the communication between known hosts.

  Authentication prevents unauthenticated devices and users from gaining access to your LAN. For 802.1X and MAC RADIUS authentication, end devices must be authenticated before they receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server.

  On a switch that is configured with both 802.1X authentication and PVLANs, when a new device is attached to the PVLAN network, the device is authenticated and then is assigned to a secondary VLAN based on the PVLAN configuration or RADIUS profile. The device then obtains an IP address and is given access to the PVLAN network.

  [See Using 802.1X Authentication and Private VLANs Together on the Same Interface.]

- **Private VLANs (EX2300 switches)**—Starting in Junos OS Release 18.2R1, you can enable private VLANs (PVLANs) on EX2300 platforms.

  PVLANs provide Layer 2 isolation between ports within a VLAN, splitting a broadcast domain into multiple discrete broadcast subdomains by creating secondary VLANs. PVLANs are useful for restricting the flow of broadcast and unknown unicast traffic and for limiting the communication between known hosts.

  [See Understanding Private VLANs.]

- **Support for DHCP snooping and other access port security features on private VLANs (EX4300 switches and Virtual Chassis)**—Starting in Junos OS Release 18.2R1, you can enable Dynamic Host Configuration Protocol (DHCP) snooping for security purposes on access ports that are in a PVLAN. You can also protect those ports with DHCP options, dynamic ARP inspection (DAI), IP source guard, and neighbor discovery inspection.

  PVLANs provide Layer 2 isolation between ports within a VLAN, splitting a broadcast domain into multiple discrete broadcast subdomains by creating secondary VLANs. PVLANs are useful for restricting the flow of broadcast and unknown unicast traffic and for limiting the communication between known hosts.

  Ethernet LANs are vulnerable to attacks such as address spoofing (forging) and Layer 2 denial of service (DoS) on network devices. The following port security features help protect access ports on your device against loss of information and productivity that such attacks can cause:

  - DHCP snooping—Filters and blocks ingress DHCP server messages on untrusted ports. DHCP snooping builds and maintains a database of DHCP lease information, which is called the DHCP snooping database.
  - DHCPv6 snooping—DHCP snooping for IPv6.
  - DHCP option 82—Also known as the DHCP Relay Agent Information option. Helps protect the switch against attacks such as spoofing of IP addresses and MAC addresses and DHCP IP address starvation.

- DHCPv6 option 37—Remote ID option for DHCPv6. Used to insert information about the network location of the remote host into DHCPv6 packets.
- DHCPv6 option 18—Circuit ID option for DHCPv6. Used to insert information about the client port into DHCPv6 packets.
- DHCPv6 option 16—Vendor ID option for DHCPv6. Used to insert information about the vendor of the client hardware into DHCPv6 packets.
- DAI—Prevents Address Resolution Protocol (ARP) spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made on the basis of the results of those comparisons.
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. The source IP address in the packet sent from an untrusted access interface is validated against the DHCP snooping database.
- IPv6 source guard—IP source guard for IPv6.
- IPv6 neighbor discovery inspection—Prevents IPv6 address spoofing attacks. Neighbor discovery requests and replies are compared against entries in the DHCPv6 snooping database, and filtering decisions are made on the basis of the results of those comparisons.

[See Putting Access Port Security on Private VLANs.]

Restoration Procedures Failure

- **Device recovery mode introduced in Junos OS with upgraded FreeBSD (EX Series)**—Starting in Junos OS Release 18.2R1, for devices running Junos OS with upgraded FreeBSD, provided you have saved a rescue configuration on the device, there is an automatic device recovery mode that goes into action should the system go into amnesiac mode. The new process is for the system to automatically retry to boot with the saved rescue configuration. In this circumstance, the system displays the banner **Device is in recovery mode** in the CLI (in both the operational and configuration modes). Previously, there was no automatic process to recover from amnesiac mode. A user with load and commit permission had to log in using the console and fix the issue in the configuration before the system would reboot.

  [See Saving a Rescue Configuration File.]

Software Installation and Upgrade

- **Phone-home client (EX2300 and EX3400 switches)**—Starting with Junos OS Release 18.2R1, you can use either the legacy DHCP-options-based ZTP or the phone-home client (PHC) to provision software for the switch. If the switch boots up and there are DHCP options received from the DHCP server for ZTP, ZTP resumes. If DHCP options are not present, PHC is attempted. PHC enables the switch to securely obtain bootstrapping data, such as a configuration or software image, with no user intervention other than having to physically connect the switch to the network. When the switch first boots, PHC connects to a redirect server, which will redirect to a phone home server to get the configuration or software image.

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

Software Licensing

- **Advanced Feature License (AFL) (EX3400 switches)**—Starting with Junos OS Release 18.2R1, the following features are available as part of the AFL:
  - Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
  - IPv6 routing protocols: IPv6 BGP and IPv6 for MBGP
  - IS-IS
  - Virtual routing and forwarding (VRF) BGP

[See Understanding Licenses for EX Series.]

System Management

- **New tool to detect high CPU utilization (EX Series)**—Starting in Junos OS Release 18.2R1, a flight recorder tool is introduced to gather historical data on when the CPU utilization on a device was high and what processes caused the high utilization. The tool collects snapshots of data enabling detection of high CPU usage and faster resolution of issues.

  Because some of the high CPU utilization cases are intentional or expected, you can enable and disable the flight recorder tool to avoid false alarms.

  [See request flight-recorder set high-cpu and show flight-recorder status.]

- **Recovering the Primary Partition (EX4300-48MP switches)**—Starting in Junos OS Release 18.2R1, the EX4300-48MP switch contains a single 50-Gigabyte SSD, which contains both the primary and backup partitions. The backup partition has a copy of the primary partition, and the backup disk partition is used to recover the primary disk partition in the event that the primary partition gets corrupted. If the primary partition gets corrupted, a notification will be logged in syslog. issues.

  If the switch is booted from the backup partition, you can recover the primary disk partition by issuing the **set system software add on-primary force-host** command.

  [See Recovering the Primary Partition on EX4300-48MP Switches .]

User Interface and Configuration

- **Support for displaying ephemeral configuration data with filtering (EX Series)**—Starting in Junos OS Release 18.2R1, the **show ephemeral-configuration** command enables you to specify the scope of the configuration data to display. To filter the displayed configuration data, append the statement path of the requested hierarchy to the command.

  [See Displaying Ephemeral Configuration Data in the Junos OS CLI.]

Virtual Chassis

- **Virtual Chassis support (EX4300-48MP)**—Starting in Junos OS Release 18.2R1, EX4300-48MP switches can be interconnected into a Virtual Chassis as one logical device managed as a single chassis. An EX4300-MP Virtual Chassis can contain up to 10 members in either of the following combinations:
  - A non-mixed Virtual Chassis if the members are all EX4300-48MP switches.
  - A mixed Virtual Chassis if the members are a combination of EX4300-48MP switches with other EX4300 switches. The mixed-mode setting is required on all switches. The members in the Routing Engine role must be EX4300-48MP switches, and other EX4300 switches can only be configured in

the linecard role. The EX4300-48MP cannot form a mixed Virtual Chassis with any other type of switches.

The 40-Gbps ports on the rear panel of EX4300-48MP switches are dedicated Virtual Chassis ports (VCPs). You must use those ports to interconnect EX4300-48MP Virtual Chassis members into a non-mixed or mixed Virtual Chassis. The dedicated VCPs cannot be converted into and used as network ports, and no other ports on the EX4300-48MP switch can be used as VCPs. In addition, EX4300 members in a mixed Virtual Chassis with EX4300-48MP members must have a special port mode enabled on VCPs to interconnect with VCPs on EX4300-48MP members. To enable this mode for all VCPs on an EX4300 switch, include the **ieee-clause-82** option when setting mixed mode on the switch, as follows:

```
user@switch> request virtual-chassis mode ieee-clause-82 mixed
```

Otherwise, configuring and administering a non-mixed or mixed mode EX4300-48MP Virtual Chassis is the same as for other EX4300 Virtual Chassis or QFX Series Virtual Chassis.

[See Understanding EX4300 Virtual Chassis.]

SEE ALSO

Changes in Behavior and Syntax

IN THIS SECTION

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 18.2R1 for the EX Series.

EVPN

- On EX9200 switches, you can configure EVPN to extend a Junos Fusion Enterprise or multichassis link aggregation group (MC-LAG) network over an MPLS network to a data center or campus network. For both Junos Fusion Enterprise and MC-LAG use cases, you must include the **bgp-peer** configuration statement in the **[edit routing-instances *name* protocols evpn mclag]** hierarchy level. This configuration enables the interworking of EVPN-MPLS with Junos Fusion Enterprise or MC-LAG. If you do not include the **bgp-peer** configuration statement in your configuration, unexpected behavior and a core dump could result. To enforce this configuration, we now check for this configuration during the commit. If the configuration is not present, an error occurs.

  See [Understanding EVPN-MPLS Interworking with Junos Fusion Enterprise and MC-LAG .]

High Availability (HA) and Resiliency

- **commit fast-synchronize** option not supported for products with single Routing Engine (EX Series)—Starting in Junos OS Release 18.2R1, Junos OS does not support the configuration option **commit fast-synchronize** at the **[edit system]** hierarchy level for all the products with single Routing Engine for which **chassis redundancy graceful-switchover** is not supported. This option is disabled from the CLI.

Interfaces and Chassis

- **EEE not supported on mge interfaces operating at 100-Mbps speed (EX2300-24MP and EX2300-48MP)**—In Junos OS Releases 18.1R2, 18.2R1, and later, if both Energy Efficient Ethernet (EEE) and 100-Mbps speed are configured on a rate-selectable (or multirate) Gigabit Ethernet (mge) port on EX2300-24MP and EX2300-48MP switches, the port operates only at 100-Mbps speed but EEE is not enabled on that port. EEE is supported only on mge interfaces that operate at 1-Gbps and 2.5-Gbps speeds.

Junos OS XML, API, and Scripting

- **Junos XML protocol <open-configuration> operation no longer emits an uncommitted changes warning (EX Series)**—Starting in Junos OS Release 18.2R1, the Junos XML protocol **<open-configuration>** operation does not emit an "**uncommitted changes will be discarded on exit**" warning message when opening a private copy of the candidate configuration. However, Junos OS still discards the uncommitted changes upon closing the private copy.

Junos Telemetry Interface

- **Change to the configuration location for gRPC-based sensor subscriptions from an external collector (EX Series)**—Starting in Junos OS Release 18.2R1, when an external streaming server, or collector, provisions sensors to export data through gRPC on devices running Junos OS, the sensor configuration is committed to the **junos-analytics** instance of the ephemeral configuration database, and the configuration can be viewed by using the **show ephemeral-configuration instance junos-analytics** operational command. In earlier releases, the sensor configuration is committed to the default instance of the ephemeral configuration database.

Layer 2 Features

- **Configuration option for LLDP VLAN name type, length, and value (TLV) (EX3400, EX4300)**—Starting in Junos OS Release 18.2R1, you can configure the **vlan-name-tlv-option (name | vlan-id)** statement at the **[edit protocols lldp]** hierarchy level to select whether to transmit the VLAN name or simply the VLAN ID for the Link Layer Discovery Protocol (LLDP) VLAN name TLV when exchanging LLDP messages. By default, EX Series switches running Enhanced Layer 2 Software (ELS) transmit the VLAN ID for the LLDP VLAN name TLV, and the **show lldp detail** command displays the default string **vlan-*vlan-id*** for an interface's VLAN name in the **Vlan-name** output field. Switches that support the **vlan-name-tlv-option** statement behave the same as the default if you configure the **vlan-id** option with this statement. If you configure the **name** option, the switch transmits the VLAN name instead, and the **show lldp detail** command displays the VLAN name in the **Vlan-name** output field.

Multicast

- **Support for per-source multicast traffic forwarding with IGMPv3 (EX4300)**—Starting in Junos OS Release 18.2R1, EX4300 switches forward multicast traffic on a per-source basis according to received IGMPv3 INCLUDE and EXCLUDE reports. In releases prior to this release, EX4300 switches process IGMPv3 reports, but instead of source-specific multicast (SSM) forwarding, they consolidate IGMPv3 INCLUDE and EXCLUDE mode reports for a group into one route for all sources sending to the group. As a result, with the prior behavior, receivers might get traffic from sources they didn't specify.

  [See IGMP Snooping Overview.]

Network Management and Monitoring

- **New context-oid option for trap-options configuration statement to distinguish the traps which come from a non-default routing instance and non-default logical system (EX Series)**—In Junos OS Release 18.2R1, a new option, **context-oid**, for the **trap-options** statement allows you to handle prefixes such as <routing-instance name>@<trap-group> or <logical-system name>/<routing-instance name>@<trap-group> as an additional varbind.

  [See trap-options.]

Software Installation and Upgrade

- **New DHCP option introduced for ZTP retry (EX Series)**—Starting in Junos OS Release 18.2R1, a new DHCP option is introduced to set the timeout value for the file downloads over FTP. If the **transfer-mode** is set as FTP, the default value for the time out is automatically set as 120 minutes. That is, if the FTP session gets interrupted due to loss of connectivity in the middle of a file transfer, it will timeout after 120 minutes and ZTP will attempt to retry the file-fetching process. This value can be overridden using the DHCP option as follows:

```
option NEW_OP.ftp-timeout code 7 = text;
option NEW_OP.ftp-timeout “val”;
```

  where **“val”** is the user configurable timeout value in seconds and must be provided (for example, “val”).

User Interface and Configuration

- **Changes to the show ephemeral-configuration command (EX Series)**—Starting in Junos OS Release 18.2R1, the **show ephemeral-configuration** operational mode command has the following changes:
  - To display the configuration data in the default instance of the ephemeral configuration database, issue the **show ephemeral-configuration instance default** command. In earlier releases, ephemeral configuration data for the default instance is displayed using the **show ephemeral-configuration** command.
  - To display the configuration data in a user-defined instance of the ephemeral configuration database, issue the **show ephemeral-configuration instance *instance-name*** command. In earlier releases, ephemeral configuration data for a user-defined instance is displayed using the **show ephemeral-configuration *instance-name*** command.
  - To view the complete post-inheritance configuration merged with the configuration data in all instances of the ephemeral database, issue the **show ephemeral-configuration merge** command. In earlier releases, the merged view is displayed using the **show ephemeral-configuration | display merge** command.
- **Change to the maximum number of user-defined instances supported by the ephemeral configuration database (EX Series)**—Starting in Junos OS Release 18.2R1, devices running Junos OS that support configuring the ephemeral configuration database enable configuring a maximum of seven user-defined instances of the ephemeral database. In earlier releases, you can configure up to eight user-defined instances. User-defined instances are configured using the **instance *instance-name*** statement at the **[edit system configuration-database ephemeral]** hierarchy level.

SEE ALSO

Known Behavior

IN THIS SECTION

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.2R1 for the EX Series.

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

General Routing

- For EX2300-24MP and EX2300-48MP, it might take 40 seconds to 50 seconds to display the correct poe oper-status when the **show poe interface** command is issued. PR1329362
- QSFP+-40G-CU3M is not supported on EX9253 switch. PR1341969
- On MGE interfaces, IEEE 802.3 clause 78 EEE is not supported with 100M speed. PR1346302

Interfaces and Chassis

- **EEE not supported on mge interfaces operating at 100-Mbps speed (EX4300-48MP)**—Starting in Junos OS Releases 18.2R1, if both Energy Efficient Ethernet (EEE) and 100-Mbps speed are configured on a rate-selectable (or multirate) Gigabit Ethernet (mge) port, the port operates only at 100-Mbps speed but EEE is not enabled on that port. Note that EEE is supported only on mge interfaces that operate at 1-Gbps, 2.5-Gbps, 5-Gbps, and 10-Gbps speeds.

SEE ALSO

New and Changed Features | 32

Changes in Behavior and Syntax | 45

Known Issues | 51

Resolved Issues | 54

Documentation Updates | 56

Migration, Upgrade, and Downgrade Instructions | 56

Product Compatibility | 58

Known Issues

IN THIS SECTION

This section lists the known issues in hardware and software in Junos OS Release 18.2R1 for the EX Series.

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

Authentication and Access Control

- DHCPv6 client is not support in this release for EX4300-48MP. PR1373691

General Routing

- The dcpfe process might crash and generate a core file if an unsupported SFP-T is put in the switch. PR1290318
- On EX4300-48-MP switch, when <cli>irb bind</cli> is committed to a VLAN without the defining IRB logical interface, the command <cli >irb bind</cli> is not committed. The IRB logical interface has to be defined before binding to VLAN. PR1342443
- Complete L2, L3 unicast traffic loss is seen on rebooting master FPC. PR1364227
- On EX4300-48MP, multiple syslog errors are seen on performing a switchover. **DELETE ERROR, Tree has a node which is neither src nor dest, flags:20if_pfe_ge_ea_incr_proc: MAC filter to be processed: 00:00:00:00:00:00** PR1365188
- A traffic drop might be seen with swap out of a VC of QFX5100 to the EX9253 for testing some heavy multicast even when IRB comes up. PR1369099
- On EX4300-48MP, the dcpfe core file is generated during NSSU upgrade from one Juniper-internal build to another Juniper-internal build. PR1369978

High Availability (HA) and Resiliency

- When **bpdu-block-on-edge** is configured, a dynamic filter update is sent to the Packet Forwarding Engine to reinstall the port bitmap. During make-before-brake (MBB) operation, a new filter entry is created first and then the old entry is deleted. With this, a noncontiguous free entry in the Packet Forwarding Engine TCAM hardware is seen. Now, when IGMP snooping is enabled, which install another set of filter update which were required to be contiguous in nature and due to previous noncontiguous free entry, the IGMP snooping filter updates are NOT programmed in orderly and contiguous fashion. Because of this, all CPU-originated IP protocol multicast traffic (OSPF, VRRP, and so on) could not be flooded out of the network ports. PR1301773

Infrastructure

- Junos OS might hang trying to acquire the SMP IPI lock while rebooting when it is running as a VM on Linux and QEMU hypervisor. PR1359339

Platform and Infrastructure

- MPC5 - inline-ka PPP echo requests are not transmitted when anchor-point is lt-x/2/x or lt-x/3/x in pseudowire deployment. PR1345727
- There is no support of interface range for channelized interfaces on EX9253, User has to configure interfaces individually. PR1350635
- 1G is not supported on uplink module in EX4300-48-MP. Inserting 1G causes MAC errors and port is removed from software linkscan, the very next insertion of any xcvr (10G in this case) fails to add the port to software linkscan resulting in the problem. Subsequent insertion of 10G xcr successfully completes the initialization. PR1374390

SEE ALSO

New and Changed Features | 32

Changes in Behavior and Syntax | 45

Known Behavior | 50

Resolved Issues | 54

Documentation Updates | 56

Migration, Upgrade, and Downgrade Instructions | 56

Product Compatibility | 58

Resolved Issues

IN THIS SECTION

This section lists the issues fixed in the Junos OS Release 18.2R1 for EX Series switches.

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

Forwarding and Sampling

- DHCP service crashes after EX9251 switch is set to factory default by zeroize. PR1329682

General Routing

- Traffic loss is observed while performing NSSU. PR1311977
- The major alarm **Fan and PSU Airflow direction mismatch** might be seen when removing the management cable. PR1327561
- A new configuration statement operational status detail statement is added in **show poe interface**. PR1330183
- The rpd process generates a core file on new backup Routing Engine at task_quit,task_terminate_timer_callback,task_timer_dispatch,task_scheduler after disabling NSR+GRES. PR1330750
- Cannot install backup Linux first when both SSD partitions are corrupted. PR1342168
- On EX2300-24MP chassis, the FAN count is incorrect in jnxFruName, jnxFilledDescr and jnxContainersCount.4. PR1361025

- On EX4300-48MP, while running regression scripts, syslog error **Error in bcm_port_sample_rate_set(ifl_cmd) : Reason Invalid port** is seen. 1376504
- IP transit traffic hits the lo0 filter. PR1379328
- In EX4300-48MP on rare occasion, when **arp-inspection** and **ip-source-guard** are configured for around 150 VLANs together, then some port might show incorrect large value for DAI statistics. PR1379443
- On rare occasions in EX4300-48MP, when **dynamic-arp-inspection**and **ip-source-guard** are removed and added back for around 150 VLANs in one go, then **arp-inspection** statistics for one of the port shows garbage value. PR1379447

Interfaces and Chassis

- On EX2300 and EX3400, IPv6 neighborship is not created on the IRB interface. PR1198482
- The interface might not work properly after FPC restarts. PR1329896

Layer 2 Features

- The DCPFE/FXPC process might crash and generate a core file. PR1362332

Layer 2 Ethernet Services

- EX Series platforms might display a false positive CB alarm **PMBus Device Fail**. PR1298612

MPLS

- A unified ISSU is not supported with MPLS configuration. PR1264786

Platform and Infrastructure

- Autonegotiation is not working as expected between EX4300 and SRX5800. PR1311458
- The FPC might crash because of the memory leak caused by the VTEP traffic. PR1356279

SEE ALSO

New and Changed Features | 32

Changes in Behavior and Syntax | 45

Known Behavior | 50

Documentation Updates

There are no errata or changes in Junos OS Release 18.2R1 documentation for the EX Series switches.

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.

NOTE: NSSU is not supported on EX2300-VC/EX3400-VC from Junos OS Release 15.1X53 to Junos OS Release 18.1R1 or later releases. For example, NSSU is not supported from Junos OS Release 15.1X53-D58 to Junos OS Release 18.1R1 or Junos OS Release 15.1X53-D57 to Junos OS Release 18.2R1

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

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

SEE ALSO

- New and Changed Features | 32
- Changes in Behavior and Syntax | 45
- Known Behavior | 50
- Known Issues | 51
- Resolved Issues | 54
- Documentation Updates | 56
- Product Compatibility | 58

Product Compatibility

IN THIS SECTION

Hardware Compatibility

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

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

Hardware Compatibility Tool

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

SEE ALSO

New and Changed Features | 32
Changes in Behavior and Syntax | 45
Known Behavior | 50
Known Issues | 51
Resolved Issues | 54
Documentation Updates | 56
Migration, Upgrade, and Downgrade Instructions | 56

Junos OS Release Notes for Junos Fusion Enterprise

IN THIS SECTION

These release notes accompany Junos OS Release 18.2R1 for Junos Fusion Enterprise. Junos Fusion Enterprise is a Junos Fusion that uses EX9200 switches in the aggregation device role. These release notes describe new and changed features, limitations, and known problems in the hardware and software.

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

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

New and Changed Features

IN THIS SECTION

This section describes the new features and enhancements to existing features in Junos OS Release 18.2R1 for Junos Fusion Enterprise.

> **NOTE:** For more information about the Junos Fusion Enterprise features, see the Junos Fusion Enterprise User Guide.

Junos Fusion Enterprise

- **Aggregation device support on EX9253 (Junos Fusion Enterprise)**—Starting with Junos OS Release 18.2R1, EX9253 switches are supported as aggregation devices in a Junos Fusion Enterprise. The aggregation device acts as the single point of management for all devices in the Junos Fusion Enterprise. Junos Fusion Enterprise supports the 802.1BR standard.

  [See Junos Fusion Enterprise Overview.]

- **Junos Fusion Enterprise support for EX4600 switches (Junos Fusion Enterprise)**—Starting with Junos OS Release 18.2R1, you can configure EX4600 switches as satellite devices in a Junos Fusion Enterprise topology. The satellite device in a Junos Fusion topology is managed and configured by the aggregation device. Junos Fusion Enterprise uses EX9200 switches in the aggregation device role.

  [See Junos Fusion Enterprise Overview.]

SEE ALSO

Changes in Behavior and Syntax | 61

Known Behavior | 61

Known Issues | 62

Resolved Issues | 63

Documentation Updates | 64

Migration, Upgrade, and Downgrade Instructions | 64

Product Compatibility | 70

Changes in Behavior and Syntax

IN THIS SECTION

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 18.2R1 for Junos Fusion Enterprise.

High Availability (HA) and Resiliency

- **commit fast-synchronize** option not supported for products with single Routing Engine (Junos Fusion Enterprise)—Starting in Junos OS Release 18.2R1, Junos OS does not support the configuration option **commit fast-synchronize** at the **[edit system]** hierarchy level for all the products with single Routing Engine for which **chassis redundancy graceful-switchover** is not supported. This option is disabled from the CLI.

SEE ALSO

New and Changed Features | 59

Known Behavior | 61

Known Issues | 62

Resolved Issues | 63

Documentation Updates | 64

Migration, Upgrade, and Downgrade Instructions | 64

Product Compatibility | 70

Known Behavior

IN THIS SECTION

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.2R1 for Junos Fusion Enterprise.

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

Junos Fusion Enterprise

- In a Junos Fusion Enterprise, it can take 6 to 30 seconds for the traffic to converge when the aggregation device is powered off or powered on. PR1257057

SEE ALSO

New and Changed Features | 59

Changes in Behavior and Syntax | 61

Known Issues | 62

Resolved Issues | 63

Documentation Updates | 64

Migration, Upgrade, and Downgrade Instructions | 64

Product Compatibility | 70

Known Issues

IN THIS SECTION

This section lists the known issues in hardware and software in Junos OS Release 18.2R1 for Junos Fusion Enterprise.

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

Junos Fusion Enterprise

- In a Junos Fusion Enterprise, it can take 6 to 30 seconds for the traffic to converge when the aggregation device is powered off or powered on. PR1257057

SEE ALSO

New and Changed Features | 59

Changes in Behavior and Syntax | 61

Known Behavior | 61

Resolved Issues | 63

Documentation Updates | 64

Migration, Upgrade, and Downgrade Instructions | 64

Product Compatibility | 70

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 18.2R1

- Mirrored packets are dropped if analyzer output extended port is reachable via the ICL link. PR1211123
- In a Junos Fusion Enterprise, an SCPD core might be seen on an aggregation device when DACL on dot1x enabled port is installed on a single homed satellite device. PR1328247
- DHCP security binding entries are not synced after the FPC comes offline or online. PR1332828
- In a Junos Fusion Enterprise, there is an issue with 802.1X re-authentication. PR1345365

SEE ALSO

New and Changed Features | 59
Changes in Behavior and Syntax | 61
Known Behavior | 61
Known Issues | 62
Documentation Updates | 64
Migration, Upgrade, and Downgrade Instructions | 64
Product Compatibility | 70

Documentation Updates

There are no errata or changes in Junos OS Release 18.2R1 for Junos Fusion Enterprise documentation.

SEE ALSO

New and Changed Features | 59
Changes in Behavior and Syntax | 61
Known Behavior | 61
Known Issues | 62
Resolved Issues | 63
Migration, Upgrade, and Downgrade Instructions | 64
Product Compatibility | 70

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Basic Procedure for Upgrading Junos OS on an Aggregation Device | 65
- Upgrading an Aggregation Device with Redundant Routing Engines | 67
- Preparing the Switch for Satellite Device Conversion | 67
- Converting a Satellite Device to a Standalone Switch | 69

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

Basic Procedure for Upgrading Junos OS on an Aggregation Device

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

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

To download and install Junos OS:

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

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

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

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

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

5. Select the **Software** tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

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

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

```
user@host> request system software add validate reboot
source/junos-install-ex92xx-x86-64-18.2R1.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-x86-64-18.2R1.n-limited.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

Preparing the Switch for Satellite Device Conversion

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

For satellite device hardware and software requirements, see Understanding Junos Fusion Enterprise Software and Hardware Requirements.

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

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

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

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

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

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

2. Clear the device:

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Switch

In the event that you need to convert a satellite device to a standalone device, you will need to install a new Junos OS software package on the satellite device and remove 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 on EEOL releases and to review a list of EEOL releases, see https://www.juniper.net/support/eol/junos.html

Downgrading from Junos OS Release 18.2

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

> **NOTE:** You cannot downgrade more than three releases.
>
> For more information, see the Installation and Upgrade Guide.

To downgrade a Junos Fusion Enterprise from Junos OS Release 18.2R1, follow the procedure for upgrading, but replace the 18.1 **junos-install** package with one that corresponds to the appropriate release.

SEE ALSO

New and Changed Features | 59

Product Compatibility

IN THIS SECTION

Hardware and Software Compatibility

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

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

Hardware Compatibility Tool

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

SEE ALSO

Junos OS Release Notes for Junos Fusion Provider Edge

IN THIS SECTION

These release notes accompany Junos OS Release 18.2R1 for the Junos Fusion Provider Edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

There are no new features or enhancements to existing features for Junos Fusion Provider Edge in Junos OS Release 18.2R1.

SEE ALSO

Changes in Behavior and Syntax

IN THIS SECTION

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 18.2R1 or later for Junos Fusion Provider Edge.

High Availability (HA) and Resiliency

- **commit fast-synchronize** option not supported for products with single Routing Engine (Junos Fusion Provider Edge)—Starting in Junos OS Release 18.2R1, Junos OS does not support the configuration option **commit fast-synchronize** at the **[edit system]** hierarchy level for all the products with single Routing Engine for which **chassis redundancy graceful-switchover** is not supported. This option is disabled from the CLI.

SEE ALSO

Known Behavior

IN THIS SECTION

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.2R1 for Junos Fusion Provider Edge.

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

Junos Fusion

- In Junos Fusion with EVPN solution when an Aggregation Device looses EVPN connectivity with rest of the Aggregation Devices then LACP over extended ports on this core isolated Aggregation Device will be brought down until EVPN connectivity is restored. PR1327784

SEE ALSO

Known Issues

IN THIS SECTION

This section lists the known issues in hardware and software in Junos OS Release 18.2R1 for Junos Fusion Provider Edge.

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

Junos Fusion

- In Junos Fusion, once the interface is marked **Loop Detect PDU Error: Detected** in the **show interface <intf_name>** command, then **clear error loop-detect interface <intf_name or all>** has to be executed on all aggregration devices to bring the interface to the up state. PR1327366

SEE ALSO

- New and Changed Features | 71
- Changes in Behavior and Syntax | 72
- Known Behavior | 73
- Resolved Issues | 75
- Documentation Updates | 76
- Migration, Upgrade, and Downgrade Instructions | 76
- Product Compatibility | 85

Resolved Issues

IN THIS SECTION

This section lists the issues fixed in the Junos OS Release 18.2R1 for Junos Fusion Provider Edge.

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

Class of Service (CoS)

- Aggregated Ethernet link-protection feature is not supported. PR1355498

Junos Fusion

- Duplicated packets might be received on the multicast downstream devices and multicast receivers. PR1316499
- In Junos fusion, the **show interfaces diagnostics optics satellite** command does not display any outputs. PR1327876
- High IGMP leave latency occurs with IGMP snooping in EVPN. PR1327980
- In Junos Fusion, an aggregate device might show a plus sign (+) sign on the ICL link for a satellite device. PR1335373

SEE ALSO

New and Changed Features | 71

Changes in Behavior and Syntax | 72

Known Behavior | 73

Known Issues | 74

Documentation Updates | 76

Migration, Upgrade, and Downgrade Instructions | 76

Product Compatibility | 85

Documentation Updates

There are no errata or changes in Junos OS Release 18.2R1 documentation for Junos Fusion Provider Edge.

SEE ALSO

New and Changed Features | 71
Changes in Behavior and Syntax | 72
Known Behavior | 73
Known Issues | 74
Resolved Issues | 75
Migration, Upgrade, and Downgrade Instructions | 76
Product Compatibility | 85

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 Provider Edge. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

Basic Procedure for Upgrading an Aggregation Device

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

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

The download and installation process for Junos OS Release 18.2R1 is different that for earlier Junos OS releases.

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

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

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

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

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

5. Select the **Software** tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

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

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

- For 64-bit software:

> **NOTE:** We highly recommend that you see 64-bit Junos OS software when implementing Junos Fusion Provider Edge.

```
user@host> request system software add validate reboot
source/jinstall64-18.2R1.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot
source/jinstall-18.2R1.SPIN-domestic-signed.tgz
```

All other customers, use the following commands.

- For 64-bit software:

> **NOTE:** We highly recommend that you see 64-bit Junos OS software when implementing Junos Fusion Provider Edge.

```
user@host> request system software add validate reboot
source/jinstall64-18.2R1.SPIN-export-signed.tgz
```

- For 32-bit software:

  ```
  user@host> request system software add validate reboot
  source/jinstall-18.2R1.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 18.2R1 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

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

Customers with EX4300 switches, use the following command:

```
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 OS that is compatible with satellite device conversion, perform the following steps:

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

2. Clear the device:

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Device

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

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

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

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

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

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

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

4. Select the Junos OS Release 14.1X53-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 once the software installation starts. The software upgrade starts after this command is entered.

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

12. When you are prompted to log back into your device, uncable the device from the Junos Fusion topology. See *Removing a Transceiver from a QFX Series Device* or *Remove a Transceiver*, as needed. Your device has been removed from Junos Fusion.

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

Upgrading an Aggregation Device

When you upgrade an aggregation device to Junos OS Release 18.2R1, 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 Release 18.2

To downgrade from Release 18.2 to another supported release, follow the procedure for upgrading, but replace the 18.2 **jinstall** package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

SEE ALSO

Product Compatibility

IN THIS SECTION

Hardware Compatibility

Hardware Compatibility

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

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

Hardware Compatibility Tool

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

SEE ALSO

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

IN THIS SECTION

These release notes accompany Junos OS Release 18.2R1 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

This section describes the new features and enhancements to existing features in Junos OS Release 18.2R1 for the MX Series routers.

Release 18.2R1-S4 New and Changed Features

Services Applications

- **Inline JFlow support for EVPN traffic (MX10008)**—Starting in Junos OS Release 18.2R1-S4, inline Jflow supports sampling under the bridge family. Inline Jflow monitors traffic hitting the bridge family and reports the necessary fields in either version 9 or IPFIX format.

  A new family **bridge** is introduced under the **[edit forwarding-options sampling instance]** hierarchy that monitors all traffic hitting the VPLS or bridge family.

  [See Understanding Inline Active Flow Monitoring.]

Release 18.2R1-S2 New and Changed Features

Routing Protocols

- **Support for IPv4 VPN unicast and IPv6 VPN unicast address families in BGP (MX Series)**—Starting with Junos OS Release 18.2R1-S2, the following address families are supported to enable advertisement and/or reception of multiple paths to a destination to/from the same BGP peer, instead of advertising/receiving only the active path to/from the same BGP peer, under [edit protocols bgp group *group-name*] hierarchy.
  - IPv4 VPN unicast (**family inet-vpn**)

- IPv6 VPN unicast (**family inet6-vpn**)

Release 18.2R1 New and Changed Features

Hardware

- **Support for JNP10K-LC2101 MPC (MX10008)**—Starting in Junos OS Release 18.2R1, Junos OS supports a new fixed-configuration MPC, JNP10K-LC2101. A fixed-configuration MPC does not contain separate slots for Modular Interface Cards (MICs). MX10008 routers support eight JNP10K-LC2101 MPCs. The JNP10K-LC2101 MPC provides a maximum bandwidth of 2.4Tbps and has six Packet Forwarding Engines, each providing a maximum bandwidth of up to 400 Gbps, which cannot be oversubscribed. You can configure the bandwidth of the MPC to provide a decreased bandwidth of 1.44Tbps as well, if required. Use the **set chassis fpc *fpc-slot-number* pfe-bandwidth *240g*** to modify the forwarding capacity of each PFE to 240 Gbps.

  JNP10K-LC2101 supports:

  - Multi-rate ports. The ports on the JNP10K-LC2101 MPC support multiple port speeds such as 10 Gbps, 40 Gbps, and 100 Gbps. Hence, they are known as multi-rate ports. All ports support all port speeds. To view the port speed information for each port, use the **show chassis pic fpc-slot *fpc-slot-number* pic-slot *pic-slot-number*** command.
  - PIC-based tunnel configuration.
  - Maximum transmission unit (MTU) size of 16,000 bytes for transit traffic.
  - Dynamic Power Management for effective utilization of available power.
  - Flexible queuing supports 128,000 queues per line card, including queues on both ingress and egress interfaces. You can use an additional license to support up to 256,000 queues or 1,500,000 queues per slot.

  See JNP10K-LC2101 MPC on MX10008 Routers Overview

- **JNP10K-LC2101 MPC (MX10008)**—Starting with Junos OS Release 18.2R1, JNP10K-LC2101 MPC is supported on the MX10008 router. The JNP10K-LC2101 MPC has fixed MPC ports with 2.4 Tbps and supports 24 100-Gigabit Ethernet QSFP28 ports, and 24 40-Gigabit Ethernet QSFP ports, and 96 10-Gigabit Ethernet ports using a breakout cable (4x10 Gigabit Ethernet). The MPC also supports combinations of 100-Gigabit Ethernet, 40-Gigabit Ethernet, and 10-Gigabit Ethernet ports.

- **New Routing and Control Board REMX2008-X8-128G (MX2008)**—Starting in Junos OS Release 18.2R1, the Routing and Control Board (RCB), REMX2008-X8-128G is supported on MX2008 routers. The RCB has increased memory and storage to support node virtualization . The RCB is equipped with an 8-Core 2.3 GHz processor, 128 GB memory, and two 200 GB SSDs and also supports Secure Boot for enhanced boot security.

  [See MX2008 Routing and Control Board (MX2008 RCB) Description.]

Authentication and Access Control

- **Enhancement to NTP authentication method (MX240, MX480, MX960, MX2020, and MX2010)**—Starting in Junos OS Release 18.2R1, Junos OS supports NTP authentication for both SHA-1 and SHA2-256, in addition to the existing NTP authentication method, MD5. You can now choose from among MD5, SHA-1, and SHA2-256 for synchronizing the clocks of Juniper Network routers, switches, and other security devices on the Internet. Using SHA-1 instead of MD5 improves the security of devices with very little impact to timing, while using SHA2-256 provides an increase in security over SHA-1.

  > **NOTE:** By default, network time synchronization is unauthenticated.

  To implement authentication, use **set authentication-key <*key_number*> type** at the **[edit system ntp]** hierarchy level.

  - To enable SHA-1 authentication, use **set authentication key <*key_number*> type sha1 value <*password*>** at the **[edit system ntp]** hierarchy level.
  - To enable SHA2-256 authentication, use **set authentication key <*key_number*> type sha256 value <*password*>** at the **[edit system ntp]** hierarchy level.

  [See authentication-key and Configuring NTP Authentication Keys]

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

- **Existing TACACS+ behavior is made VRF aware (MX Series)**—Starting in Junos OS Release 18.2R1, the **routing-instance** statement at the **[edit system tacplus-server *server-address*]** hierarchy level and **[edit system accounting destination tacplus server server-address]** hierarchy level can now be used to configure any routing instance present under the **[edit routing-instances]** hierarchy level. TACACS+ traffic uses the configured routing instance, whatever the name. Before, the **routing-instance** statement at the **[edit system tacplus-server *server-address*]** hierarchy level and **[edit system accounting destination tacplus server server-address]** hierarchy level could be used only to configure the mgmt_junos routing instance.

  [See Configuring TACACS+ Authentication and Configuring TACACS+ System Accounting.]

Class of Service (CoS)

- **Support for collecting aggregate queue statistics for underlying logical interfaces (MX Series)**—By default to preserve memory resources, aggregate queue statistics are not collected for underlying logical interfaces (Level 2 interfaces). Queue statistics are only collected for the upper-level logical interfaces (Level 3 and above) and the physical interface (Level 1). By default the command **show interfaces queue *interface-name*** shows all zeroes for underlying logical interfaces. Starting with Junos OS Release 18.2R1, you can enable the collection of aggregate queue statistics for all underlying logical interfaces on a particular physical or aggregate (for example, ae0) interface by enabling **logical-interface-aggregate-statistics** at the **[edit class-of-service interfaces *interface-name*]** hierarchy

level. You can show the aggregate queue statistics by running the **show interfaces queue *interface-name*** command.

[See logical-interface-aggregate-statistics.]

- **Support for excluding the overhead bytes from queue statistics (MX Series)**—By default, the Layer 2 header bytes applied to upper-level logical interfaces are included in CoS per-queue statistics at the physical interface, which can provide inaccurate results. Starting with Junos OS Release 18.2R1, you can exclude the counting of overhead bytes from aggregate queue statistics by enabling **exclude-queue-overhead-bytes** option at the **[edit class-of-service interfaces *interface-name*]** hierarchy level. To also exclude the counting of overhead bytes from aggregate queue statistics of all child interfaces, including logical interfaces and interface sets, add the **include-hierarchy** option at the **[edit class-of-service interfaces *interface-name* exclude-queue-overhead-bytes]** hierarchy level.

  [See exclude-queue-overhead-bytes.]

- **Support for bypass-queuing-chip option (vMX)**—Starting with Junos OS Release 18.2R1, the **bypass-queuing-chip** option at the **[edit class-of-service interfaces *interface-name*]** hierarchy level is supported on vMX routers. Enable this option on vMX routers to save a vCPU when scheduling is not needed on an interface. With this option, be careful not to oversubscribe the interface bandwidth.

  [See bypass-queuing-chip.]

EVPN

- **NOTE:** This feature is documented but not supported in Junos OS Release 18.2R1

  NSR and unified ISSU support for point-to-multipoint LSP for EVPN provider tunnel (MX Series and vMX)—Starting in Junos OS Release 18.2R1, Junos OS provides nonstop routing (NSR) and unified ISSU support for point-to-multipoint (P2MP) inclusive provider tunnels. This ensures that broadcast, unknown unicast, and multicast (BUM) packets continue after a Routing Engine switchover occurs when NSR is enabled.

  NOTE: Unified ISSU is not supported on the vMX routers.

  [See *Understanding P2MPs LSP for the EVPN Inclusive Provider Tunnel*.]

- **Support for EVPN-VPWS flexible cross-connect (MX Series)**—Starting with Junos OS Release 18.2R1, Ethernet VPN (EVPN) virtual private wire service (VPWS) flexible cross-connect is introduced to address a label resource issue that could occur on some low end access routers. This is possible when there are a group of attachment circuits (ACs) under the same EVPN instance (EVI) and share the same label.

> **NOTE:** The label resource issue is applicable to a service edge router that is interoperable with the access router that uses FXC scheme to conserve its label usage. It is assumed that the label resource issue does not apply to Juniper Networks service edge router, the vMX (or MX), that uses the pseudowire subscriber interface. Thus there is no change for the label assign scheme on the service edge router with regular EVPN-VPWS pseudowire subscriber head-end termination.

[See Overview of Flexible Cross-Connect Support on VPWS with EVPN.]

- **Support for head-end termination for EVPN VPWS for business services (MX Series)**—Starting with Junos OS Release 18.2R1, Ethernet VPN (EVPN) virtual private wire service (VPWS) is supported on pseudowire subscriber logical interface.

  Prior to Junos OS 18.2 Release, pseudowire subscriber logical interface is used with either Layer 2 circuit or Layer 2 VPN for psuedowire headend termination service.

  An Ethernet VPN (EVPN) enables you to connect dispersed customer sites using a Layer 2 virtual bridge. Virtual private wire service (VPWS) Layer 2 VPNs employ Layer 2 services over MPLS to build a topology of point-to-point connections that connect end customer sites in a VPN. EVPN-VPWS as a next generation of pseudowire subscriber interface technology brings the benefit of EVPN to point-to-point service by providing fast convergence upon node failure and link failure through its multihoming feature. As a result, you can use EVPN-VPWS on pseudowire subscriber interface for head-end termination into different services.

  You can configure the pseudowire subscriber logical interface for EVPN-VPWS so that the pseudowire established by EVPN-VPWS can be headend terminated into either Layer 3 VPN or BGP-VPLS. The head-end termination covers single (single-homed) pseudowire termination and redundant (multihomed) pseudowire termination into Layer 3 VPN and BGP-VPLS.

  [See Overview of Pseudowire Subscriber Logical Interface Support on VPWS with EVPN.]

- **EVPN pure type-5 route support (MX Series)**—Starting with Junos OS Release 18.2R1, you can configure pure type-5 routing in an Ethernet VPN (EVPN) Virtual Extensible LAN (VXLAN) environment. Pure type-5 routing is used when the Layer 2 domain does not exist at the remote data centers. A pure type-5 route advertises the summary IP prefix and includes a BGP extended community called a router MAC, which is used to carry the MAC address of the sending switch and to provide next-hop reachability for the prefix. To configure pure type-5 routing, include the **ip-prefix-routes advertise direct-nexthop** statement at the **[edit routing-instances *routing-instance-name* protocols evpn]** hierarchy level. To enable two-level equal-cost multipath (ECMP) next hops in an EVPN-VXLAN overlay network, you must also include the **overlay-ecmp** statement at the **[edit forwarding-options vxlan-routing]** hierarchy level.

  [See Understanding EVPN Pure Route Type-5.]

- **IGMP snooping support for EVPN-MPLS (MX Series, vMX)**—Starting with Junos OS Release 18.2R1, you can configure IGMP snooping on MX Series routers with MPCs and vMX routers in an Ethernet

VPN (EVPN) over an MPLS network. Enabling IGMP snooping helps to constrain multicast traffic to interested receivers in a broadcast domain.

Multicast sources and receivers in the EVPN instance (EVI) can each be single-homed to one provider edge (PE) device or multihomed (in all-active mode only) to multiple PE devices. When IGMP snooping is configured with multihomed receivers, IGMP state information is synchronized among peer PE devices by exchanging BGP EVPN Type 7 (Join Sync Route) and Type 8 (Leave Sync Route) network layer reachability information (NLRI). When PE devices receive multicast traffic from the EVPN core on a multihomed Ethernet segment (ES), only the designated forwarder (DF) PE device forwards the traffic, and the DF forwards the traffic only to interested receivers (selective multicast forwarding) based on IGMP snooping reports and BGP EVPN Type 7 routes. PE devices serving single-homed receivers also use selective multicast forwarding based on IGMP snooping reports to forward the traffic only to interested receivers, conserving network bandwidth.

All PE devices perform inclusive multicast forwarding using ingress replication to forward multicast traffic into the EVPN core to reach all remote PE devices. Multicast traffic at Layer 3 is routed between bridge domains or VLANs using IRB interfaces.

This feature is supported with multiple EVIs, multicast sources and receivers on the same or different sites, and IGMP snooping in proxy mode only.

To enable IGMP snooping on PE devices in an EVPN instance, include the **igmp-snooping proxy** statement at the [**edit routing-instances *routing-instance-name* protocols**] or the [**edit routing-instances *routing-instance-name* bridge-domain *bridge-domain-name* protocols**] hierarchy level.

For inter-VLAN multicast forwarding, PIM distributed DR (PIM DDR) mode must be enabled on all participating IRBs.

EVPN and IGMP snooping operational mode commands can be used to view information learned from IGMP snooping messages or EVPN Type 7 and Type 8 messages.

[See Overview of Multicast Forwarding with IGMP Snooping in an EVPN-MPLS Environment.]

- **NOTE:** This feature is documented but not supported in Junos OS Release 18.2R1

Support for mLDP P2MP tunnels with EVPN for BUM traffic (MX Series and vMX)—Although present in the code, the ability to configure and signal a P2MP LSP for the EVPN inclusive provider tunnel for BUM traffic is not supported in Junos OS Release 18.2R1. P2MP LSPs manages efficient core bandwidth utilization because it uses multicast replication only at the required nodes instead of ingress replication at the ingress PE node.

- **Support for OSPF, IS-IS, BGP, and static routing on IRB interfaces in EVPN-VXLAN networks (MX Series and vMX)**—Starting in Junos OS Release 18.2R1, you can configure OSPF, IS-IS, BGP, and static routing with bidirectional forwarding detection (BFD) on an IRB interface that is used as a routed interface in EVPN. This allows protocol adjacencies to be established between an IRB on a Layer 3 gateway and

a CE device connected directly to a Layer 3 gateway or to a Layer 2 leaf device in an EVPN-VXLAN network.

[See Supported Protocols on an IRB Interface in EVPN-VXLAN .]

- **Support for groupVPN failover to backup router (MX Series and vMX)**—Group VPN is a trusted group to eliminate point-to-point tunnels and their associated overlay routing. All group members share a common security association (SA), known as a group SA (GSA). The GSA enables group members to decrypt traffic that was encrypted by any other group member. Starting in Junos OS Release 18.2R1, Junos OS confirms the Group VPN redundancy with service redundancy daemon running on MX Series routers. MX Series routers with redundancy between them act as Group VPN members.
- **Support for passing of traffic during a policy mismatch between key server and group member (MX Series and vMX)**—Currently, packets that do not match the traffic policy provided by the group key server are dropped by default. Starting in Junos OS Release 18.2R1, you have an option to change the default behavior to disable encryption and forward the packets instead of dropping them.

  You can configure the **forward-policy-mismatch** within the **group vpn object** configuration to enable the support for forwarding policy-mismatched packets at the **[edit security group-vpn member ipsec]** hierarchy level.

- **NOTE:** This feature is documented but not supported in Junos OS Release 18.2R1

  EVPN P2MP bud router support (MX Series and vMX)—Starting in Junos OS Release 18.2R1, Junos OS supports configuring a point-to-multipoint (P2MP) label switched path (LSP) as a provider tunnel on a bud router. The bud router functions both as an egress router and a transit router.

  To enable a bud router to support P2MP LSP, include the **evpn p2mp-bud-support** statement at the **[edit routing-instances routing-instance-name protocols evpn]** hierarchy level.

  [See Configuring Bud Node Support]

Flow-Based and Packet-Based Processing

- **Support for inline flow monitoring (MX10008)**—Starting in Junos OS Release 18.2R1, Junos OS supports inline active flow monitoring. Inline active flow monitoring supports version 9 and IPFIX flow collection templates. Version 9 template is supported for IPv4, IPv6, MPLS, and MPLS-IPv4. IPFIX template is supported for IPv4, IPv6, MPLS, MPLS-IPv4, and VPLS flows. Both IPFIX and version 9 templates use UDP as the transport protocol.

  [See Inline Active Flow Monitoring.]

High Availability (HA) and Resiliency

- **Resiliency support for JNP10K-LC2101 MPC (MX10008)**—Starting in Junos OS Release 18.2R1, resiliency support is enabled for JNP10K-LC2101 MPC on MX10008 routers.

Interfaces and Chassis

- **Enhancement to increase the threshold of corrected single-bit errors (MPC7E, MPC8E, MPC9E on MX Series)**—In Junos OS Release 18.2R1, the threshold of corrected single-bit errors is increased from 32 to 1024, and the alarm severity is changed from Major to Minor for those error messages. There is no operational impact upon corrected single-bit errors. Also, a log message is added to display how many single-bit errors have been corrected between the reported events as follows:

  EA[0:0]: HMCIF Rx: Link0: Corrected single bit errordetected in HMC 0 - Total count 25

  EA[0:0]: HMCIF Rx: Link0: Corrected single bit errordetected in HMC 0 - Total count 26

  [See Alarm Overview.]

- **Fabric management support (MX10008)—**Starting in Junos OS Release 18.2R1, fabric management is supported on MX10008 routers. The fabric architecture of MX10008 routers consists of six Switch Fabric Boards (SFBs). The MX10008 MPC has six Packet Forwarding Engines, each having 24 connections to the fabric (24 fabric planes, or 4 connections per SFB). The MX10008 will have 24 planes active when all the six SFBs are populated. However, in case of a failure of one SFB, line rate can still be achieved with 20 planes (that is, a minimum of five SFBs are required to achieve line rate). The fabric supports a link speed of 25 Gbps. Fabric management involves training the fabric links, monitoring the links, and collecting fabric statistics. The MX10008 also supports fabric hardening.

  [See Fabric Plane Management on JNP10K-LC2101 Overview]

- **Support for FRU control, power management, and environmental monitoring (MX10008)**—Starting with Junos OS Release 18.2R1, Junos OS chassis management software for MX10008 routers with JNP10K-LC2101 MPC provides enhanced environmental monitoring and FRU control. MX10008 has a pair of Routing Engines, which support virtualization. Each Routing Engine board is a single FRU. All FRUs including Routing Engines, Packet Forwarding Engines, interfaces, power supplies, and fan trays are upgradable. The MX10008 chassis supports two kinds of power supply modules (PSM)—a DC PSM and an AC PSM. The AC PSM delivers 2700 W of power, while the DC PSM delivers 2500 W. The MX10008 cooling system contains two fan trays, with 11 fans in each fan tray. MX10008 supports temperature thresholds for each temperature sensor, which enables the router to precisely control the

cooling, raise alarms, and shut down a FRU. The router also supports preserving power-on sequence for the FPCs.

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

- **Support for inline Two-Way Active Measurement Protocol (TWAMP) server and client on MX10008—** Starting in Junos OS Release 18.2R1, Mx10008 router with MPC7E cards support the inline Two-Way Active Measurement Protocol (TWAMP) control-client and server for transmission of TWAMP IPv4 UDP probes between the session-sender (control-client) and the session-reflector (server). The TWAMP control-client and server can also work with a third-party server and control-client implementation.

  TWAMP is an open protocol for measuring network performance between any two devices that support TWAMP. To configure the TWAMP server, specify the logical interface on the service PIC that provides the TWAMP service by including the twamp-server statement at the: **[edit interfaces si-fpc/pic/ port unit logical-unit-number rpm]** hierarchy level.

  To configure the TWAMP client, include the twamp-client statement at the: **[edit interfaces si-fpc/pic/ port unit logical-unit-number rpm]** hierarchy level.

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

- **Software support for MX10008—**Starting in Junos OS Release 18.2R1, MX10008 routers support the following software features:
  - Class of services (CoS)—Helps prioritize packets to avoid random loss of data when a network experiences congestion and delay.
  - Tunneling and encryption—Encapsulates arbitrary packets inside a transport protocol; and thereby provides a private, secure path through an otherwise public network.
  - Firewall filters—Provide rules that define whether to accept or discard packets that are transiting an interface.
  - Port mirroring—Enables you to analyze traffic on routers and switches that, unlike hubs, do not broadcast packets to every port on the destination device.
  - OpenConfig—Supports the use of vendor-neutral data models to configure and manage the network.
  - Detection of wedge condition—Detects several types of wedge conditions. A wedge condition is caused by an error that blocks network traffic.
  - Junos Telemetry Interface (JTI)—Enables you to provision sensors to collect and export data for various system resources, such as physical interfaces and firewall filters.

- **Limited encryption Junos OS image and boot restriction (MX2008)—**Starting with Junos OS Release 18.2R1, the MX2008 routers with the Routing Engines REMX2008-X8-64G-LT support only the Junos Limited image. The Junos Limited image does not have data-plane encryption and is intended only for countries in the Eurasian Customs Union because these countries have import restrictions on software containing data-plane encryption. Unlike the Junos Worldwide image, the Junos Limited image supports control-plane encryption through SSH and SSL, thus allowing secure management of the system. The Routing Engines are restricted to boot only the Junos Limited image.

[See Junos OS Editions.]

- **Support for secure boot and upgraded SSD size and RAM size (MX2008)—**Starting in Junos OS Release 18.2R1, a significant system security enhancement, secure boot, has been introduced. The Secure Boot implementation is based on the UEFI 2.4 standard. The BIOS has been hardened and serves as a core root of trust. The BIOS updates, the boot loader, and the kernel are cryptographically protected. No action is required to implement secure boot.

  The SSD size and the RAM size of the REMX2008-X8-128G-S Routing Engine is upgraded to 2x200-GB and 128-GB, respectively.

  [See Feature Explorer and enter **Secure Boot**.]

- **Upgraded SSD size and RAM size on the REMX200-8-X8-128G-S Routing Engine (MX2008)—** Starting in Junos OS Release 18.2R1, the SSD size and the RAM size of the REMX2008-X8-128G-S Routing Engine are upgraded to 2x200-GB and 128-GB, respectively. The increased SSD size facilitates increased storage of core and log files.

  [See Salient Features of the Routing Engines with VM Host Support.]

- **Support for 240-V high-voltage DC (HVDC) PSMs and PDMs (MX2008, MX2010, MX2020)**—Starting in Junos OS Release 18.2R1, Junos OS supports 240-V HVDC power supply modules (PSMs; model number: MX2K-PSM-DC-240V) and power distribution modules (PDMs; model number: MX2K-PDM-DC-240V) on the MX2000 line of routers. The PDM supplies 240-V HVDC power to each PSM. The 240-V HVDC power supplies are similar in functionality and physical specifications to the existing DC PSMs and PDMs supported on the MX2000 routers, except that the 240-V HVDC PSMs and PDMs support 240-V input voltage feed. The 240-V HVDC PSMs and PDMs are supported in HVDC environments that support an input voltage range of 190 VDC through 290 VDC.

- **Support for PTP over Ethernet and hybrid mode over link aggregation group (MX240, MX480, MX960, MX2010, MX2020)**—Starting in Junos OS Release 18.2R1, the MPC5E and MPC6E line cards support Precision Time Protocol (PTP) over Ethernet and hybrid mode over a link aggregation group (LAG).

  Link aggregation is a mechanism of combining multiple physical links into a single virtual link to achieve linear increase in bandwidth and to provide redundancy in case a link fails. The virtual link is referred to as an aggregated Ethernet interface or a LAG.

  [See Precision Time Protocol Overview]

Junos Telemetry Interface

- **Streaming OpenConfig data from Routing Engine (RE) sensors over UDP in protobuf format (MX)**–Starting in Junos OS Release 18.2R1, you can stream OpenConfig-based sensor data from Routing Engine sensors using the Junos Telemetry Interface (JTI). This allows you to stream the OpenConfig sensor data in gRPC/protobuf format rather than in key/value pairs. This makes the messages smaller and is more efficient.

  [See Overview of the Junos Telemetry Interface.]

- **Routing Engine state sensors for the Junos Telemetry Interface (MX Series)**—Starting with Junos OS Release 18.2R1, you can export statistics for the Routing Engine state through the Junos Telemetry Interface using the following resource paths:

  - **/junos/kernel-ifstate/stats/churn-rate**
  - **/junos/kernel-ifstate/stats/peer-consumption-rate**
  - **/junos/kernel-ifstate/stats/vetos-statistics**

  Only gRPC streaming is supported.

  To provision the sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module.

  Support for the Junos Telemetry Interface was introduced on QFX10000 and QFX5200 switches in Junos OS Release 17.2R1.

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

- **Expanded ON_CHANGE support for Junos Telemetry Interface (JTI) (MX Series)**—Starting with Junos OS Release 18.2R1, OpenConfig support through remote procedure call (RPC) and JTI is extended to support additional ON_CHANGE sensors.

  Periodical streaming of OpenConfig operational states and counters collects information at regular intervals. ON_CHANGE support streams operational states as events (only when there is a change), and is preferred over periodic streaming for time-sensitive missions.

  These paths, previously supporting periodical streaming only, now also support ON_CHANGE streaming:

  - **/interfaces/interface/state/admin-status**
  - **/interfaces/interface/state/description**
  - **/interfaces/interface/state/oper-status**
  - **/interfaces/interface/subinterfaces/subinterface/state/admin-status**
  - **/interfaces/interface/subinterfaces/subinterface/state/description**
  - **/interfaces/interface/subinterfaces/subinterface/state/oper-status**
  - **/interfaces/interface/subinterfaces/subinterface/state/ifIndex**

- **/interfaces/interface/subinterfaces/subinterface/state/index**
- **/interfaces/interface/subinterfaces/subinterface/state/name**

These resource paths from the preceding list do not change with an event, but will be streamed on creation and deletion:

- **/interfaces/interface/subinterfaces/subinterface/state/ifIndex**
- **/interfaces/interface/subinterfaces/subinterface/state/index**
- **/interfaces/interface/subinterfaces/subinterface/state/name**

To provision a sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module.

To enable ON_CHANGE support, configure the sample frequency in the subscription as zero. When you create a subscription using a top-level container as the resource path (for example, **/interface**), leaf devices under the resource path **/interface** with ON_CHANGE support are automatically streamed based on events. Other leaf devices will not be streamed.

Before events are streamed, there is an initial stream of states to the collector, followed by an **END_OF_INITIAL_SYNC**. This notice signals the start of event streaming.

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

- **J-Insight Device Monitor (MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, and vMX)**–J-Insight is a data-driven device monitoring solution that provides visibility and insight into the health of a running system. Starting with Junos OS Release 18.2R1, the J-Insight framework facilitates real-time monitoring of system resources for FPC FRUs. It also has been integrated with the existing connectivity error management infrastructure to normalize error detection, monitoring, and reporting. J-Insight is an on-premise system application that uses the Junos Telemetry Interface to continuously collect data that is reflective of the current state and health of the device component being monitored.

  [See J-Insight Device Monitor Overview.]

- **Service set and sessions support for Junos Telemetry Interface (JTI) (MX Series with MS-MICs and MS-MPCs)**—Starting with Junos OS Release 18.2R1, you can export service set and sessions statistics. These sensors provide visibility for IPsec services on different service complexes and nodes.

  Exported data is defined using an IP address and a UDP port. When an export interval expires, the most recent statistics collected by the sensors are gathered, placed in the payload of a UDP packet, and forwarded to a collector. A timestamp indicating when counters are read is included with the exported data to allow collectors to collate data. The timestamp also can determine if and when an event happened, such as a PIC hardware restart or if counters were cleared by means of the CLI.

  The following paths are supported:

  - **/junos/services/spu/servicesets/**

- **/junos/services/spu/sessions/**

For streaming statistics through UDP, all parameters are configured at the **[edit services analytics]** hierarchy level.

[See sensor and Configuring a Junos Telemetry Interface Sensor (CLI Procedure).]

Layer 2 Features

- **Support for Layer 2 and Layer 3 features (MX10008)—**Starting in Junos OS Release 18.2R1, MX10008 routers support the following Layer 2 and Layer 3 features:
  - Layer 2 protocols including Layer 2 Ethernet OAM and virtual private LAN service (VPLS)
  - Integrated routing and bridging (IRB)
  - Multichassis link aggregation groups (MC-LAGs)
  - Layer 3 routing protocols and MPLS
  - Inline BFD
  - Multicast

  [See Layer 2 and Layer 3 Features on MX Series Routers]

Layer 3 Features

- **Multipoint support for ATM MIC with SFP (MX Series routers with MPCs and ATM MIC with SFP)**—Starting in Junos OS Release 18.2R1, MX Series routers with an ATM MIC (model number MIC-3D-8OC3-2OC12-ATM) with SFP can communicate with multiple devices through ATM links. With this multipoint support feature, ATM MIC can communicate with multiple Layer 3 peers in the ATM network. In earlier Junos OS releases, the ATM MIC communicates only with one Layer 3 peer.

  On an ATM MIC, the following configurations are required for multipoint support:

  - Configure the **multipoint** option at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level to communicate with multiple Layer 3 peers on ATM interface.
  - Configure the **multipoint-destination** option with its corresponding **vci** at the **[edit interfaces *interface-name* unit *logical-unit-number* family *family* address *address*]** hierarchy to enable multipoint support on ATM interface.

    The **Inverse-arp** configuration option is an optional configuration to enable inverse ARP for **multipoint-destination** at the **[edit interfaces at-fpc/pic/port unit logical-unit-number family family address address multipoint-destination address]** hierarchy level. Only responding to inverse ARP request is supported. Generation of Inverse ARP is not supported.

  [See Configuring a Point-to-Multipoint Connection on ATM MICs.]

MPLS

- **Interoperability of segment routing with LDP (MX Series)**—In an LDP network with gradual deployment of segment routing, some devices may not support segment routing, which can cause interoperability

issues in the network. Starting in Junos OS Release 18.2R1, you can use OSPF or ISIS to enable segment routing devices to operate with the LDP devices that are not segment routing capable.

To implement this feature using OSPF, an extended prefix link-state advertisement (LSA) with Range type, length, and value (TLV) for all the LDP prefixes is generated, and mapping routes corresponding to the prefix is installed in the inet.3 and mpls.0 routing tables.

To implement this feature using ISIS, a server-client configuration is required under protocols ISIS and LDP, respectively, and routes from the inet.3 or inet.0 routing tables are used for stitching of segment routing LSP with an LDP LSP and vice-versa.

[See LDP Mapping Server for Interoperability of Segment Routing with LDP Overview.]

- **Support for reporting binding SIDs to a PCE (MX Series)**—Static non-colored segment routing LSPs have binding segment identifiers (SIDs) that are used for stitching multiple non-colored segment routing LSPs. Junos OS supports a maximum of five next hops for provisioning such segment routing LSPs.

  Starting in Junos OS Release 18.2R1, statically configured non-colored segment routing LSPs on the ingress device are reported to the Path Computation Element (PCE) through a Path Computation Element Protocol (PCEP) session. These non-colored segment routing LSPs may have binding SID labels associated with them.

  With this feature, the PCE can use this binding SID label in the label stack to provision PCE-initiated segment routing LSP paths.

  [See Static Segment Routing Label Switched Path.]

Network Management and Monitoring

- **SNMP MIB and trap support for group VPN members (MX Series)**—Starting in Junos OS Release 18.2R1, an SNMP MIB (jnxGdoiMIB) is added under jnxMibs, which is based on the GDOI MIB draft, draft-kamarthy-gdoi-mib-01. This MIB provides the SNMP MIB tables and notifications required for group VPN members. SNMP **get**, **get_next**, and **walk** functionality is added to the following tables:

  - jnxGdoiGroupTable
  - jnxGdoiGmTable
  - jnxGdoiGmKekTable
  - jnxGdoiGmTekSelectorTable
  - jnxGdoiGmTekPolicyTable

  Also, SNMP trap notifications are provided for the following events:

  - jnxGdoiGmRegister
  - jnxGdoiGmRegistrationComplete
  - jnxGdoiGmReRegister

- jnxGdoiGmRekeyReceived
- jnxGdoiGmRekeyFailure

[See MIB Explorer and Standard SNMP MIBs Supported by Junos OS]

- **RPM timestamping extension on JNP10K-LC2101 (MX10008)**—Starting in Junos OS Release 18.2R1, JNP10K-LC2101 supports timestamping of RPM probes in the Packet Forwarding Engine host processer. You can enable this feature by including the **hardware-timestamp** statement at the [edit services rpm probe probe-name test test-name] hierarchy level.

  [See hardware-timestamp].

- **Support for RPM probes with IPv6 sources and destinations on JNP10K-LC2101 (MX10008)**—Starting in Junos OS Release 18.2R1, the RPM client router (the device that originates the RPM probes) can send probe packets to the RPM probe server (the device that receives the RPM probes) that contains an IPv6 address. To specify the destination IPv6 address used for the probes, include the **target (url *ipv6-url* | address *ipv6-address*)** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. You can also define the RPM client or the source that sends RPM probes to contain an IPv6 address. To specify the IPv6 protocol-related settings and the source IPv6 address of the client from which the RPM probes are sent, include the **inet6-options source-address *ipv6-address*** statement at the **[edit services rpm probe owner test test-name]** hierarchy level.

- **Support for specifying a maximum hop count for RPM and TWAMP probes (MX Series routers)**—Starting in Junos OS Release 18.2R1, you can set a maximum hop count (TTL) for real-time performance monitoring (RPM) probes (both IPv4 and IPv6). This can be useful, for example, to restrict the scope of a given RPM probe so it cannot unintentionally monitor an alternative path to the destination, such as may occur following a BGP rerouting. Probes that exceed the number set for TTL are discarded.

  This TTL configuration is supported on Routing Engine-based RPM, MS-MPC based RPM, MS-MIC-based RPM, and Two-Way Active Management Protocol (TWAMP).

  [See RPM Overview and TTL (RPM probe).]

Restoration Procedures and Failure Handling

- **Device recovery mode introduced in Junos OS with upgraded FreeBSD (MX Series)**—Starting in Junos OS Release 16.1R1, for devices running Junos OS with upgraded FreeBSD, provided you have saved a rescue configuration on the device, there is an automatic device recovery mode that goes into action should the system go into amnesiac mode. The new process is for the system to automatically retry to boot with the saved rescue configuration. In this circumstance, the system displays the banner **Device is in recovery mode** in the CLI (in both the operational and configuration modes). Previously, there was no automatic process to recover from amnesiac mode. A user with load and commit permission had to log in using the console and fix the issue in the configuration before the system would reboot.

  [See Saving a Rescue Configuration File.]

Routing Protocols

- **Topology-independent loop-free alternate for OSPF (MX Series)**—Starting in Junos OS Release 18.2R1, topology-independent loop-free alternate (TI-LFA) with segment routing provides MPLS fast reroute (FRR) backup paths corresponding to the post-convergence path for a given failure. You can enable TI-LFA for OSPF by configuring the **use-post-convergence-lfa** statement at the **[edit protocols ospf backup-spf-options]** hierarchy level. When used with OSPF, TI-LFA provides protection against link failure and node failure.

  You can enable the creation of post-convergence backup paths for a given interface by configuring the **post-convergence-lfa** statement at the **[edit protocols ospf 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 ospf area *area* interface *interface-name* post-convergence-lfa]** hierarchy level.

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

- **Support for route leaking in OSPF stub areas (MX Series)**—Starting with Junos OS Release 18.2R1, route leaking is supported in OSPF when the router is overloaded, which allows redistribution of the external prefixes.

  Prior to Junos OS Release 18.2 , the external prefixes are not redistributed when OSPF is overloaded.

  You can now configure the following when OSPF is overloaded.

  - **allow-route-leaking** at the **[edit protocols <ospf | ospf3> overload]** hierarchy level to advertise the external prefixes with maximum cost.
  - **stub-network** at the **[edit protocols ospf overload]** hierarchy level to advertise stub network with maximum metric.
  - **intra-area-prefix** at the **[edit protocols ospf3 overload]** hierarchy level to advertise intra-area prefix with maximum metric.
  - **as-external** at the **[edit protocols <ospf | ospf3> overload]** hierarchy level to advertise external prefix with maximum metric.

  [See Understanding OSPF Overload Function.]

Services Applications

- **Traffic Load Balancer enhancements (MX Series with MS-MPCs)**—Starting in Junos OS Release 18.2R1, the Traffic Load Balancer (TLB) application supports the following enhancements:
  - 2000 TLB instances for virtual services that use the direct-server-return or translated mode
  - Tracing at the instance level or at the virtual services level
  - Display of real server up and down counts

  [See Configuring TLB.]
- **Port Control Protocol support for DS-Lite on MS-MPCs and MS-MICs (MX Series routers)**—Starting in Junos OS Release 18.2R1, Port Control Protocol (PCP) on the MS-MPC and MS-MIC supports DS-Lite. PCP provides a mechanism to control the forwarding of incoming packets by upstream devices such as NAT44 and firewall devices, and a mechanism to reduce application keepalive traffic.

  [See Port Control Protocol Overview.]
- **IKE and IPsec enhancements on MS-MPCs and MS-MICs (MX Series routers)**—Starting in Junos OS Release 18.2R1, the following enhancements are supported on MS-MPCs and MS-MICs:
  - You can configure the MX Series router to act only as an IKE responder. In this responder-only mode, the MX Series router does not initiate IKE negotiations, it only responds to IKE negotiations initiated by the peer gateway.
  - You can configure the MX Series router to send only the end-entity certificate for certificate-based IKE authentication instead of the full certificate chain. This avoids IKE fragmentation.
  - You can display the total elapsed time for a tunnel across security association rekeys (**Total uptime**) and the configured hard lifetime for a security association (**SA lifetime**) by running the **show services ipsec-vpn ipsec security-associations detail** command.

  [See Configuring IKE Activation Time, Configuring IPsec Service Sets, and show services ipsec-vpn ipsec security-associations.]
- **Support for additional DS-Lite features on MS-MPCs and MS-MICs (MX Series routers)**—Starting in Junos OS Release 18.2R1, dual-stack lite (DS-Lite) running on MS-MPCs and MS-MICs adds support for the following features:
  - SIP ALG
  - Subscriber session limitation per subnet
  - DS-Lite service sets on AMS interfaces

  [See DS-Lite Subnet Limitation.]
- **Support of IPv6 probes for optimized CLI configuration of RPM tests (MX Series)**—Starting in Junos OS Release 18.2R1, you can also optimize the CLI configuration for RPM tests with IPv6 probes. Prior to Junos OS Release 18.2R1, you could only optimize the CLI configuration for RPM tests with IPv4

probes. Enter the **rpm-scale** statement at the **[edit services rpm probe *probe-owner* test *test-name*]** hierarchy level to generate multiple tests from a single configuration.

[See Configuring RPM Probes.]

- **Inline JFlow support for EVPN traffic (MX Series)**— Starting in Junos OS Release 18.2R1, inline jflow supports sampling under the bridge family. Inline Jflow monitors traffic hitting the bridge family and reports the necessary fields in either version 9 or IPFIX format.

  A new family **bridge** is introduced under the **forwarding-options sampling instance** hierarchy that monitors all traffic hitting the VPLS or bridge family.

  [See Understanding Inline Active Flow Monitoring.]

Software Installation and Upgrade

- **ZTP support is added for MX VM host platforms (MX Series)**—In Junos OS Release 18.2R1, ZTP, which automates the provisioning of the device configuration and software image with minimal manual intervention, is supported on MX Series VM hosts. When you physically connect a supported device to the network and boot it with a factory configuration, the device attempts to upgrade the Junos OS software image automatically and autoinstall a configuration provided on the DHCP server.

  [See Zero Touch Provisioning.]

- **Unified ISSU support (MX10003)**—Starting in Junos OS Release 18.2R1, MX10003 routers support unified in-service software upgrade (ISSU). Unified ISSU enables you to upgrade from a particular Junos OS release to a later one with no disruption on the control plane and with minimal disruption of traffic. MX10003 supports unified ISSU upgrade of the complete package including VMHOST Linux. Use the command **request vmhost software in-service-upgrade** to perform a unified ISSU upgrade. [See Understanding the Unified ISSU Process]

  NOTE:
  - Starting in Junos OS Releases 18.2R1, MX10003 supports unified ISSU.
  - MX10003 does not support upgrading only the Junos OS image using the **request system software in-service-upgrade** command.
  - Unified ISSU is not supported on MACsec MIC (JNP-MIC1-MACSEC).
  - Unified ISSU is not supported for the interfaces that are configured with 1-Gigabit Ethernet mode.
  - Unified ISSU is not supported on timing protocols (for example, Precision Time Protocol and Synchronous Ethernet), MACsec protocols, and BBE protocols.
  - The **MAC statistics** (retrieved using the show interfaces extensive command) are reset during unified ISSU which means that the **MAC statistics** command does not provide the correct statistics after unified ISSU.

Subscriber Management and Services

- **Local authentication and authorization for subscribers (MX Series)**—Starting in Junos OS Release 18.2R1, you can enable local authentication and limited local authorization for individual subscribers instead of using external authentication and authorization servers. To enable local authentication, specify the **password** option of the **authentication-order** statement in the access profile. Define the local password for the subscriber with the **password** option of the **subscriber *username*** statement in the access profile. You can configure up to 100 subscribers for local authentication chassis-wide. You can optionally configure local authorization with other options of the **subscriber *username*** statement. Local authentication statistics are displayed by the **show network-access aaa statistics authentication detail** and **show network-access requests statistics** commands.

  [See Configuring Local Authentication and Authorization for Subscribers.]

- **Nonterminating filter actions next-ip and next-ip6 supported in dynamic profiles (MX Series)**—Starting in Junos OS Release 18.2R1, the firewall filter actions **next-ip** and **next-ip6** are available in dynamic profiles. Already supported for static profiles, these nonterminating actions direct packets matching a given filter to the specified IPv4 or IPv6 destination address. When the filters including these actions are in dynamic service profiles, you can create user-defined variables to parameterize the associated address and the optional routing instance name.

  [See Parameterized Filter Nonterminating and Terminating Actions and Modifiers.]

- **Automatic validation of DHCPv6 client MAC addresses to reduce session hijacking (MX Series)**—Starting in Junos OS Release 18.2R1, the DHCPv6 local server and relay agent automatically attempt to validate a client's MAC address to prevent accepting packets from malicious clients that attempt to hijack the client session.

  When DHCPv6 local servers and relay agents receive a solicit message from a client to establish a session, they extract the client MAC address (link-layer address) from the message and add it to a local table that maps MAC addresses to client IPv6 addresses or prefixes. They use this table to compare MAC addresses received in subsequent messages from the client to validate whether the client is known; if not, it is assumed to be malicious and the control packet is dropped. Because the packet has failed MAC validation, the client MAC validation counter is incremented.

  [See DHCPv6 Client MAC Address Validation to Prevent Session Hijacking.]

- **DHCP short-cycle protection to reduce excess loading (MX Series)**—Starting in Junos OS Release 18.2R1, you can enable the router to identify DHCP clients that have short logins or continually fail to connect; the router then drops subsequent requests from these clients until a lockout timer expires. For users that repeatedly log in frequently and briefly, the initial lockout time is short enough to have no noticeable impact. As these brief logins continue, the lockout time is exponentially increased.

  [See DHCP Short Cycle Protection Against Frequent Brief or Failed Client Sessions.]

- **Support for direct PCC rule activation by a PCRF (MX Series with MS-MPCs)**—Starting in Junos OS Release 18.2R1, a policy and charging rules function (PCRF) server can directly activate a policy and charging control (PCC) rule that is configured on the MX Series router. To activate a PCC rule, the PCRF sends a Rule-Install-Name AVP over the Gx interface to the MX Series router. PCC rules define the

treatment to apply to subscriber traffic (for example, setting the maximum bit rate) based on the application being used by the subscriber (for example, Facebook) or based on the Layer 3 and Layer 4 service data flow information for the IP flow (for example, the source and destination IP addresses).

[See Configuring Application-Aware Policy Control for Subscriber Management.]

- **Dynamic profile enhancements to support migration of static, terminated IPv4 PPP subscribers (MX Series)**—Starting in Junos OS Release 18.2R1, the following enhancements support dynamic profiles for static subscribers:
  - CPE-sourced subscriber address—You can direct jpppd to use the IP address supplied by the client in an incoming IPCP configure-request message rather than assigning another address by configuring your RADIUS server to Framed-IP-Address attribute (8) with the wildcard value of 255.255.255.255.
  - Tag2 for static routes—For PPP subscribers that use static routes with a tag2 attribute for MP-BGP, you can configure your RADIUS server to include the tag2 attribute in the Framed-Route attribute [22] when it authenticates a subscriber. Alternatively, you can configure the dynamic profile to provide a specific tag2 value for a specific access route prefix.
  - Local authentication—For clients that do not support authentication protocols such as PAP and CHAP, you can configure usernames and passwords locally. You can define the name based on one or more of the following: MAC address, agent circuit identifier, agent remote identifier, and domain name. The router uses these values when it contacts the RADIUS server for authentication.

  [See Migrating Static PPP Subscriber Configurations to Dynamic Profiles Overview.]

- **Support for multipoint LDP to utilize distributed IGMP to signal an MPLS-based core has been added to Enhanced Subscriber Management (single-chassis MX Series routers with MPC2E, MPC3E, MPC5E, or MPC7E)**—Starting in Junos OS Release 18.2R1, support for multipoint LDP inband signaling to interwork with distributed IGMP has been added. As such, two separate PIM domains can be interconnected by an MPLS-based core (that is, a PIM-free core). One application of multipoint LDP inband signalling is to carry IPTV multicast traffic on an MPLS backbone.

  To enable the interworking, **chassis network-services enhanced-ip** must first be configured. Then you need to set the **igmp** or **mld** interface for **distributed**, and enable **mldp-inband-signalling** at the PIM hierarchy so PIM acts as a multipoint LDP inband edge router:

  ```
  [edit dynamic-profiles profile-name protocols igmp|mld interface layer 3 interface name distributed]
  [edit protocols pim mldp-inband-signalling]
  ```

  You can the run the **show pim source** command to confirm that distributed multipoint LDP is working (look for **Upstream neighbor via MLDP-inband**).

  [See Understanding Distributed IGMP and Enhanced Subscriber Management Overview]

- **BNG support for cascading DSLAM deployments over bonded DSL channels (MX Series)**— Starting in Junos OS Release 18.2R1, Passive Optical Network (PON) access technologies are supported with four levels of quality-of-service (QoS) scheduler hierarchy for residential subscribers in a BBE deployment. This feature extends the Access Node Control Protocol (ANCP) implementation to handle network

configuration for residential customers that use PON as the broadband access technology for both CuTTB and FTTB. ANCP uses a statically controlled traffic-control profile on the interface-set for shaping at the subscriber level at the intermediate node to which the subscribers are connected. New DSL types are provided to support access line rate adjustment for the new access technologies.

[See Understanding BNG Support for Cascading DSLAM Deployments Over Bonded DSL Channels

[See access-line (Access Line Rate Adjustment).]

A new RADIUS VSA, **inner-tag-protocol-id** 26-211 is introduced to fetch the inner VLAN Tag Protocol Identifier value for L2BSA subscribers to enable maintaining one dynamic profile instead of two separate dynamic profiles. A new Junos OS dynamic profile variable *$junos-inner-vlan-tag-protocol-id* allows a VLAN map's **inner-tag-protocol-id** to be set by RADIUS or a predefined default value provided in the configuration.

[See Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs.]

- **Global range setting for initial router advertisement intervals (MX Series)**—Starting in Junos OS Release 18.2R1, you can configure override options to set a global range from which the router randomly selects an interval for each interface for only the initial three router advertisements that the router sends when the router becomes available on that interface. This enables you to set a range that results in a very short interval for these advertisements without affecting subsequent advertisements set by the router.

  In earlier releases, you can configure an interval range only per interface and the range settings apply to all router advertisements that the router sends.

  [See Configuring an Interval Range for Unsolicited Router Advertisements to IPv6 Neighbors.]

User Interface and Configuration

- **Support for displaying ephemeral configuration data with filtering (MX Series)**—Starting in Junos OS Release 18.2R1, the **show ephemeral-configuration** command enables you to specify the scope of the configuration data to display. To filter the displayed configuration data, append the statement path of the requested hierarchy to the command.

  [See Displaying Ephemeral Configuration Data in the Junos OS CLI.]

VPN

- **Increased number of supported routing instances (MX 960 and MX 2020)**—Starting in Junos OS Release 18.2R1, Junos OS supports up to 16,000 VPLS routing instances with 128,000 (FEC 128) hierarchical VPLS pseudowires.

  [See Configuring VPLS Routing Instances.]

SEE ALSO

Changes in Behavior and Syntax | **108**

Changes in Behavior and Syntax

IN THIS SECTION

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 18.2R1 for MX Series..

EVPN

- **Change in the output for show evpn instance and show evpn database**—Starting in Junos OS Release 18.2R1, the output for **show evpn instance** and **show evpn database** displays a local interface with an interface name of .local..*number*. and no configuration. This interface is created to support configuration fault management (CFM). For example, **show evpn instance** displays the following sample output:

```
Number of local interfaces: 2 (2 up)
    Interface name  ESI                             Mode             Status
AC-Role
    .local..9       00:00:00:00:00:00:00:00:00:00  single-homed     Up
Root
```

General Routing

- **No error codes displayed for PFE errors (MX Series)**—Starting in Junos OS Release 18.2R1, on MX Series routers, the **show chassis alarms** output does not display error codes for Packet Forwarding Engine -related errors. You can use the following commands to view more details of the errors that caused the alarms:
  - **show chassis errors active**

- **show chassis errors active detail**

High Availability (HA) and Resiliency

- **commit fast-synchronize** option not supported for products with single Routing Engine (MX Series)—Starting in Junos OS Release 18.2R1, Junos OS does not support the configuration option **commit fast-synchronize** at the **[edit system]** hierarchy level for all the products with single Routing Engine for which **chassis redundancy graceful-switchover** is not supported. This option is disabled from the CLI.

Interfaces and Chassis

- On MX Series routers with the RE-S-X6-64G and RE-MX2K-X8-64G Routing Engines, when the user changes the router configuration on a live system, or when the user deletes an interface that has active traffic, the message **select: protocol failure in circuit setup** is randomly displayed. However, there is no known functional impact.

Junos OS XML API and Scripting

- **Junos XML protocol <open-configuration> operation no longer emits an uncommitted changes warning (MX Series)**—Starting in Junos OS Release 18.2R1, the Junos XML protocol **<open-configuration>** operation does not emit an "**uncommitted changes will be discarded on exit**" warning message when opening a private copy of the candidate configuration. However, Junos OS still discards the uncommitted changes upon closing the private copy.

Junos Telemetry Interface

- **Change to the configuration location for gRPC-based sensor subscriptions from an external collector (MX Series)**—Starting in Junos OS Release 18.2R1, when an external streaming server, or collector, provisions sensors to export data through gRPC on devices running Junos OS, the sensor configuration is committed to the **junos-analytics** instance of the ephemeral configuration database, and the configuration can be viewed by using the **show ephemeral-configuration instance junos-analytics** operational command. In earlier releases, the sensor configuration is committed to the default instance of the ephemeral configuration database.

MPLS

- **Display of Route Session-ID count in the show rsvp version command output**—Starting in Junos OS Release 16.1, the **show rsvp version** command output displays the **Route Session-ID count** output field

by default, even when there are no session IDs associated with the RSVP ingress routes. In such cases, the **Route Session-ID count** value is zero (0).

- **Support for inet.0 and inet.3 labeled unicast BGP route for protocol LDP (MX Series)**— Starting in Junos OS Release 18.2R1, LDP egress policy is supported on both inet.0 and inet.3 routing Information bases (RIBs) also known as routing table for labeled unicast BGP routes. If a routing policy is configured with a specific (inet.0 and inet.3) RIB, the egress policy is applied on the specified RIB. If no RIB is specified and a prefix is present on both inet.0 and inet.3 RIBs for labeled unicast BGP routes, then inet.3 RIB is preferred. However, prior to Junos OS Release 12.3R1 and starting with Junos OS Release 16.1R1, LDP egress policy is always preferred on inet.0 RIB and support for inet.3 RIB egress policy for labeled unicast BGP routes was disabled. In Junos OS Release 12.3R1 and later releases up to Junos Release 16.1R1, LDP egress policy was supported in inet.3 RIBs, in addition to inet.0 RIBs, for labeled-unicast BGP routes.

Network Management and Monitoring

- Starting in Junos OS Release 18.2R1, there must be no space in the password for configuring the Network Time Protocol (NTP) authentication-key. For example **user@host# set system ntp authentication-key 10 type md5 value "ABCDjuniper"**.

  Prior to Junos OS Release 18.2R1, the NTP authentication or password was successfully configured with a space added in the password. For example **user@host# set system ntp authentication-key 10 type md5 value "ABCD juniper"**.

- **New context-oid option for trap-options configuration statement to distinguish the traps which come from a non-default routing instance and non-default logical system (MX Series)**—In Junos OS Release 18.2R1, a new option, **context-oid**, for the **trap-options** statement allows you to handle prefixes such as <routing-instance name>@<trap-group> or <logical-system name>/<routing-instance name>@<trap-group> as an additional varbind.

  [See trap-options.]

- A decrease in the MPLS label-switched path (LSP) statistics pauses the SNMP MIB **mplsLspInfoAggrOctets** count for one MPLS statistics gathering interval. In such cases, the **mplsLspInfoAggrOctets** value is updated only after completing one more interval of the MPLS statistics gathering.

Software Installation and Upgrade

- **New DHCP option introduced for ZTP retry (MX Series)**—Starting in Junos OS Release 18.2R1, a new DHCP option is introduced to set the timeout value for the file downloads over FTP. If the **transfer-mode** is set as FTP, the default value for the timeout is automatically set as 120 minutes. That is, if the FTP session gets interrupted due to loss of connectivity in the middle of a file transfer, it will time out after 120 minutes and ZTP will attempt to retry the file-fetching process. This value can be overridden using the DHCP option as follows:

```
option NEW_OP.ftp-timeout code 7 = text;
option NEW_OP.ftp-timeout “val”;
```

where **“val”** is the user configurable timeout value in seconds and must be provided within quotes (for example,"val”).

- **ZTP is supported on MX PPC platforms (MX Series)**—As of Junos OS Release 18.2R1, zero touch provisioning (ZTP) is supported on MX PPC platforms (which are MX5, MX10, MX40, MX80, and MX104 routers). Before the fix, the ZTP process did not start to load image and configuration for MX PPC routers.

  [See Junos OS Installation Package Names.]

Subscriber Management and Services

- **Wildcard supported for show subscribers agent-circuit-identifier command (MX Series)**—Starting in Junos OS Release 18.2R1, you can specify either the complete ACI string or a substring when you issue the **show subscribers agent-circuit-identifier** command. To specify a substring, you must enter characters that form the beginning of the string, followed by an asterisk (*) as a wildcard to substitute for the remainder of the string. The wildcard can be used only at the end of the specified substring.

  [See show subscribers.]

- **Changed behavior for framed routes without a subnet mask (MX Series)**—Starting in Junos OS Release 18.2R1, the router connects the session but ignores a framed route when it is received from RADIUS in the Framed-Route attribute (22) without a subnet mask.

  In earlier releases, the router installs the framed route with a Class A, B, or C subnet mask depending on the value of the first octet. When the octet < 128, the mask is /8; when 128 <= octet < 192, the mask is /16; and when the octet >= 192, the mask is 24.

User Interface and Configuration

- **Changes to the show ephemeral-configuration command (MX Series)**—Starting in Junos OS Release 18.2R1, the **show ephemeral-configuration** operational mode command has the following changes:
  - To display the configuration data in the default instance of the ephemeral configuration database, issue the **show ephemeral-configuration instance default** command. In earlier releases, ephemeral configuration data for the default instance is displayed using the **show ephemeral-configuration** command.
  - To display the configuration data in a user-defined instance of the ephemeral configuration database, issue the **show ephemeral-configuration instance *instance-name*** command. In earlier releases, ephemeral configuration data for a user-defined instance is displayed using the **show ephemeral-configuration *instance-name*** command.

  - To view the complete post-inheritance configuration merged with the configuration data in all instances of the ephemeral database, issue the **show ephemeral-configuration merge** command. In earlier releases, the merged view is displayed using the **show ephemeral-configuration | display merge** command.

- **Change to the maximum number of user-defined instances supported by the ephemeral configuration database (MX Series)**—Starting in Junos OS Release 18.2R1, devices running Junos OS that support configuring the ephemeral configuration database enable configuring a maximum of seven user-defined instances of the ephemeral database. In earlier releases, you can configure up to eight user-defined instances. User-defined instances are configured using the **instance *instance-name*** statement at the **[edit system configuration-database ephemeral]** hierarchy level.

SEE ALSO

New and Changed Features | **87**

Known Behavior | **113**

Known Issues | **117**

Resolved Issues | **126**

Documentation Updates | **145**

Migration, Upgrade, and Downgrade Instructions | **145**

Product Compatibility | **152**

Known Behavior

IN THIS SECTION

This section contains the known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.2R1 for MX 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

- Source-prefix filtering and protocol filtering of the CGNAT sessions are incorrect. For example, **show services sessions extensive protocol udp source-prefix <0:7000::2>** displays incorrect filtering of the sessions. PR1179922
- Support for enterprise profile is only provided for 10-Gigabit Ethernet interfaces. Use of 40-Gigabit Ethernet and 100-Gigabit Ethernet interfaces might result in a phase alignment issue. PR1310048
- Sometimes 1-Gigabit Ethernet interface might remain down after certain events. Events that could cause 1-Gigabit Ethernet interface to remain down are as follows:
  - Two are interfaces connected on a loopback on 12 port QSFP28 TIC on an MX10003 or on a 4 Port QSPF28 fixed PIC on an MX204 and configured as 1-Gigabit Ethernet interfaces.
  - Two MX10003 devices are connected back to back and rebooted at the same time with 1-Gigabit Ethernet interfaces on a 12-port QSFP28 TIC.PR1312403
- Memory optimizations were done in carrier-grade NAT to increase the per session memory usage as in Junos OS Release 17.4R2 and the fix was committed through this PR. With the fix, scaling numbers are improved and 6M sessions are established. But the given fix is not enough to maintain 6M scaling sessions across other releases starting in Junos OS 18.1 Release. In these releases, PCP related RLI and many other RLI changes also have gone in. These changes have resulted in reduction in base memory and hence memory per session is decreased. Further per session memory utilization optimization in NAT is difficult through the PR. So we need collective effort from CGNAT services as well infra side to optimize it further. As per current scenario we cannot support more than 5.5 M sessions with APP/EIM/EIF enabled. PR1328510
- When a packet enters an FTI tunnel, copying the inner packet's TTL into the outer header implies that any subsequent packet drop inside the tunnel is conveyed to the source of the original packet. This is not handled in the Packet Forwarding Engine currently. So the inner packet TTL is not copied to the outer encapsulated packet header. PR1338467
- QSFP+-40G-CU3M is not supported on MX10003 router. PR1341969
- After disabling the laser for CWDM optics, optics diagnostics will not report o/p power low and laser current low alarm/warnings. PR1349258

EVPN

- In scaled up EVPN VPWS configurations(approximately 8000 EVPN VPWS), during a Routing Engine switchover, rpd scheduler slip messages might be seen. PR1225153

Forwarding and Sampling

- On an I-chip that for an IP->MPLS case, the PTYPE is carried over a fabric as an IP address, but the egress MPLS features such as filters are not executed. So traffic will not reach the hit MPLS filter and matches in Inet filter PR751618
- Root Cause of the Problem: ++++++++++++++++++++++++++ As per the investigation from RPD : we have is an interface for a direct route starting in ifdown condition. The remote side is then brought up, so I/F goes to ifup. Since it is a direct route, rpd does not install the route or nexthop. It receives that info from the kernel, and just updates a nexthop in rpd local storage. route and nexthop for the interface are taken care of in the kernel. There is no route change in rpd. route_record depends on route flash to find out about updates. Since there is no route change, there is no route flash, so route_record is blissfully unaware. In order to change this, we would need to decide that we want a route flash for this case. Currently, for direct and local routes / nexthops, these are "don't care" in rpd, as far as route updates go. We just update our nexthop info, without marking for any other notifications. A complication for the solution is a change that was done for PR 1002287, where if the NOTINSTALL flag is set, do not send the update to srrd. That flag is set for direct and local routes. Incidentally, this is day-one operation. If the interface is up at startup, it should all work correctly. FIB table can provide OIF/GW only. SRC_MASK, DST_MASK, SRC_AS and DST_AS are not available in PFE FIB Table. So SRRD connection is required. Listening to both SRRD and FIB table, and consolidating information will complicate implementation. Scanning entire FIB Table just for the few such routes will have performance impact and will complicate present implementation. This is day 1 implementation for SRRD/Sampled. Workarounds: ++++++++++++ There are two possible workarounds 1) Have the far end interface up when the DUT interface is brought up. In the case where that is not happening, a recovery would be to disable the DUT interface, then enable it again. At that point, everything should be initially brought up in the state we are looking for. 2) Enable the nexthop-learning command. Please refer to the documentation for information on this command. PR1224105

Interfaces and Chassis

- In case of hw-assisted-pm mode of operation at responder, it takes few ms/sec (based on the programmed scale) to program inline-responder entries once CCM comes up. So until inline-entry corresponding to a SLM session doesn't get programmed a response will not be send back to the originator and originator will see a loss. Once an inline-responder entry gets programmed responses will be sent back to the originator. PR1311963
- At JDM install time, each JDM instance generates pseudo random MAC addresses to be used for JDM's own management interface and for the associated GNFs' management interfaces. At GNF creation time,

each GNF instance generates pseudo random MAC addresses to be used as the chassis MAC address pool for the forwarding interfaces of that GNF. Once generated, JDM and GNF MAC addresses are persistent, and will only be deleted when the JDM or GNF instance itself is deleted.

At a GNF, the Junos OS CLI command **show chassis mac-addresses** can be used to examine its chassis MAC address pool, and the Junos OS CLI command **show interfaces fxp0** can be used to examine the MAC address of its management interface.

At JDM, the CLI command **show interfaces jmgmt0** can be used to examine the MAC address of its management interface.

In case of MAC address duplication across JDM or GNF instances, you must delete and then reinstall the respective JDM or GNF instance and check again for duplication.

- In MX10008 routers, the fabric is referred to as either Switch Interface Board (SIB) or Switch Fabric Boards (SFBs). The **show chassis hardware** output uses both SIB and SFB to refer to the fabric. The outputs of the commands **show chassis sfb errors** and **show chassis alarms** use SIB to refer to the fabric.

Routing Protocols

- Continuous soft core files might be generated due to a bgp-path-selection code. The routing protocol process (rpd) forks a child and the child asserts to produce a core file. The problem is with route-ordering and it is auto-corrected after collecting the soft-assert-core file, without any impact to the traffic or service. PR815146
- When a Junos OS aggregation gateway uses a IPv6address as a nexthop for IPv4aggregates announced to the downstream, it may attract traffic prematurely before Packet Forwarding Engines are programmed with more specific IPv4 routes. This happens when the IPv6 address is advertised in BGP inet6-labeled-unicast family. PR1220235
- Degradation is seen in BGP v4/v6 RE delete time when compared with 17.2R1 PR1289582

Services Applications

- We recommend that you do not configure **ms- interface** when AMS bundle in one-to-one mode has the same member interface. PR1209660

SEE ALSO

New and Changed Features | **87**

Changes in Behavior and Syntax | **108**

Known Issues | **117**

Resolved Issues | **126**

Known Issues

IN THIS SECTION

This section lists the known issues in hardware and software in Junos OS Release 18.2R1 for the MX Series.

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

EVPN

- L2-learning process (l2-ald) might generate a core file in a scaled Layer 2 setup, including bridge domain, VPLS, EVPN, and so on. The l2-ald process follows a kernel page. In most cases, the problem resolves on its own after an l2-ald core file is generated. In some cases, a manual restart of the process is required for recovery. PR1142719
- If a host is multihomed to a set of PE devices for redundancy, when the host's MAC or IP address is learned by one of these PE devices, then all PE devices belonging to this redundant set will install the /32 host route pointing to its local IRB interface in the tenant's IP routing instance table as long as its local multihoming ES interface connecting to this host is up . This is the optimized behavior that can be

achieved with the configuration statement routing-option forwarding-table chained-composite-next-hop ingress evpn on a QFX5110 platform unless this configuration statement is a part of the Junos OS default configuration. Otherwise, without enabling this configuration statement, if a PE device is attached to the multihomed ES learned by this host's MAC or IP address only from the control plane through EVPN, the PE device installs the /32 host route pointing to the remote PE device where it learned the host's MAC or IP address. For a PE device attached to the multihomed ES and learned by this host's MAC or IP address locally through the data plane, the PE device always installs the /32 host route pointed to its local IRB interface. PR1321187

- When VTEP scale of more than 200 is used in Junos OS Release 18.1R1, VTEPs might not come up for all the tunnels and might impact traffic. PR1342175
- On platforms running Junos OS, the l2ald daemon might crash when MAC address processing. The MAC learning process will be impacted during the period of l2ald crash. The l2ald will recover itself. PR1347606
- Bi-direction L2 traffic floods for around 5 seconds for streams from SH to MH, when **clear mac table** command is executed on MX Series because of MACs getting populated in the system taking time. The **clear mac table** is a disruptive command, which deletes all dynamic MACs in the system. PR1360348

Forwarding and Sampling

- When a policing filter is applied to an active LSP carrying traffic, the LSP resignals and drops traffic for approximately 2 seconds. It can take up to 30 seconds for the LSP to come up under the following conditions:
  - Creation of a policing filter and a policing filter application to the LSP through configuration occurs in the same commit sequence.
  - Load override of a configuration file that has a policing filter and a policing filter application to the LSP is followed by a commit. PR1160669
- Heap memory leaks occur on DPC when the flow specification route is changed. PR1305977
- This issue affects unified ISSU only when filter lists are being used. If you are upgrading from Junos OS Release 15.1F5, 15.1F6, 16.1R1, or later to Junos OS Release 17.1R2, 17.1R3, 17.2R2, 17.2X75-D50, 17.3R1 , or later, then an error with firewall can occur that will prevent firewall configuration changes from being properly applied. As a workaround, to avoid this issue, explicitly set the filter-list-template or no-filter list-template flag before doing unified ISSU. This configuration is at the top of the filters being used in filter lists (for example, **set firewall family inet filter <name> filter-list-template**).PR1345711
- When a logical interface (IFL) is operationally down, the accounting records for that IFL will not be written. PR1348249

General Routing

- In a scaled setup, remnant routes might be seen in the old master Routing Engine after Routing Engine switchover a non-GRES scenario because the rpd process in the old master Routing Engine might not have enough time to clean all the routes from kernel. In this case, there will be a convergence delay (in minutes) while the backup Routing Engine becomes master again. The length of the delay depends on the number of routes (for example, a 6M routes environment with ~1M remnant routes might have a 6-minute delay). PR1075404
- Various common situations lead to different views of forwarding information between kernel and Packet Forwarding Engines. For example, **fpc7 KERNEL/PFE APP=NH OUT OF SYNC: error code 3 REASON: NH add received for an ifl that does not exist ERROR-SPECIFIC INFO: nh_id=562 , type = Hold, ifl index 334 does not exist TYPE-SPECIFIC INFO: none.** There is no service impact observed in MPC2 and MPC3 type cards. PR1205593
- When hybrid timing mode is configured (PTPoE+SyncE), the MX Series router does not interoperate with ACX Series routers in native VLAN mode. PR1076666
- There is no configuration shown when showing default groups of junos-defaults. PR1201380
- SMID daemon has stopped responding to the management requests after a jl2tpd (L2TP daemon) crash on an MX960 BNG. PR1205546
- When an MPC is removed while the card is online, the Link Error column in the **show chassis fabric summary** extended output shows YES for all fabric planes. When the MPC is taken offline using the CLI command, output shows correctly. PR1214611
- Errors such as **mspmand[190]: msvcs_session_send: Plugin id 3 not present in the svc chain for session** are seen. They are usually cosmetic. PR1258970
- Multiple vulnerabilities exist in stunnel; Refer to https://kb.juniper.net/JSA10852for more information. PR1226804
- Sometimes when PPPoE subscribers log in and log out from Junos OS 16.1 releases, the following messages are generated: **user@devcie> show log messages | match authd authd[5208]: sdb_app_access_line_entry_read_by_uifl: uifl key 'demux0.xxxxxxxx': snapshot failed (-7) authd[5208]: sdb_app_access_line_entry_read: uifl key 'demux0.xxxxxxxx': read failed**. These messages indicate that the authd daemon for subscriber authentication is attempting to read private data for an underlying interface that no longer exists (-7 = SDB_DATA_NOT_FOUND). These messages have no impact and can be safely ignored. PR1236211
- Errors such as **mspmand[190]: msvcs_session_send: Plugin id 3** are not present in the switched virtual circuit (svc) chain for a session . They are usually cosmetic. PR1258970
- This issue occurs when an interface comes online and both OAM protocol and MKA protocol try to establish their respective sessions. Because of contention between these two protocols, OAM takes down the interface and MKA fails to establish connection (because the interface is down, it cannot send out MKA packets). PR1265352

- This very specific issue occurs when the Packet Forwarding Engine is oversubscribed with unknown unicast flood with no MAC learning, which is not a common configuration. During unified ISSU, only the Packet Forwarding Engine gets wedged. However, this issue is not seen when the Packet Forwarding Engine is oversubscribed with L3 traffic or with L2 traffic with MAC learning. PR1265898
- On MPC2E-NG, MPC3E-NG, MPC5E, MPC6E, MPC7E, MPC8E and MPC9E cards, a firewall performance feature "fast-lookup-filter" can be activated. Due to a transient parity error, the packet will be dropped within the Packet Processing Engine with a **sync xtxn error** message. This issue will affect traffic, which may eventually affect the service. PR1266879
- DEP does not support dh group group19, encryption algorithm aes-256-cbc and hash sha-384 in its list of default proposals. These must be configured explicitly in the configuration. PR1269160
- If a VM host snapshot is taken on an alternate disk and there is no further VM Host software image upgrade, if the current VM Host image gets corrupted, system will boot with an alternate disk so as user can recover primary disk to restore the state. However, if the corruption is associated with the host root file system, the node boots with the initial VM Host software instead of from the alternate disk. PR1281554
- Due to a vendor code limitation, ungraceful removing of MX10003 MACsec TIC from the chassis might cause a crash or an unpredictable result. PR1284040
- At reboot, RHEL 7.3 servers report **libvirtd[6282]: segfault at 10 ip 00007f87eab09bd0**. No core file is left and no operational impact is known. PR1287808
- A race condition exists in which the Ubuntu-based external server G-ARP might not be sent from the jmgmt0 interface, resulting in loss of connectivity to management IP of JDM. PR1291836
- Junos OS releases with a fix committed in Junos OS Releases 15.1R5-S4, 16.1R4-S3, 16.1R5, and 17.3R1 with XM-based line cards (MPC3E/4E/5E/6E/2E-NG/3E-NG) might report a **DDR3 TEMP ALARM** chassisd error log message. PR1293543
- A PCI Device missing alarm might appear when both the master and backup Routing Engine run different versions of Junos OS. This PR intents to add the ability to verify if it is related to hardware or not before generating the alarm. PR1301191
- The lo0.0 interface should be used in default VRF for subscriber services. PR1303254
- The **show dynamic-tunnels database summary** command does not show accurate tunnels summary when the anchor Packet Forwarding Engine line card is not in the up state. As a workaround, use **show dynamic-tunnels database** and **show dynamic-tunnels database terse** commands.PR1314763.
- On all MX Series platforms, if the Point-to-Point Protocol over Ethernet (PPPoE) subscribers runs on Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC) over dual-tagged VLAN and auto-sensed VLANs, all the packets that are being sent to the L2TP Network Server (LNS) might be dropped, because the LAC Ethernet pads the PPPoE packets with larger size. PR1315009
- Alarm is raised if mixed AC PEMs are present. The criteria has been changed to check whether mixed AC is present. If the PEM is AC (high) first bit of pem_voltage is set and if it is AC (low) second bit of pem_voltage is set. So if both first and second bit are set, then mixed AC is present. PR1315577

- In JDM, (running on a secondary server) the jdmd daemon might generate a core file if the GNF add-image is aborted by pressing Ctrl-C. PR1321803
- BGP-signal tunnels are always next-hop-based tunnels. The GRE tunnels created dynamically by BGP-signal are always next-hop-based, even if the user has configured the static tunnels created by GRE to use a logical interface (IFL) base. PR1322941
- With **commit full**, na-grpd daemon might restart, causing disconnect of streaming telemetry. PR1326366
- With regards to FPC restarts and Virtual Chassis splits, the design of MX Series Virtual Chassis (MX-VC) infra relies on the integrity of the TCP connections and failure situations be handled gracefully. For example, a TCP connection timeout because of jlock crossing boundary value (5 seconds) can cause bad consequences in MX-VC currently no easy solutions exist that would be able to reduce this jlock overuse besides enabling marker infra in MX-VC setup. Unfortunately, there is no immediate plan to enable the marker, because doing so causes several issues. PR1332765
- Filters configured with **scale-optimized** having the action pointing to **traffic-class-count** will not increment. PR1334580
- If unit 0 under the MS interface is defined, unit 0's logical interface (IFL) will handle exporting sampling records regardless of what you have defined as the source address under the sampling configuration. So the rules are if both a nonzero unit is used (unit 20 as an example) and an MS unit 0 is also defined, then:
  - MS unit 0 interface has to be defined with family inet because sampling records will be exported via this IFL no matter if the source-address sits under unit 20.
  - MS unit 0 interface should be part of the default routing table. There is no additional configuration required for this. By default, the interface will be in the default routing table. Also the route toward the collector should be available in the default routing table. If a nonzero unit is used and ms unit 0 is not defined then the following events occur:

    The export makes use of .local (instead of MS unit 0, as MS unit 0 is not defined) to send out the packet.

    b. Route to the collector should be available in the default routing table. PR1334682
- With certificate hierarchy, where intermediate CA profiles are not present on the device, in some corner cases, the PKI daemon can become busy and stop responding. PR1336733
- The hash value generated for 256-bit key length of AES-GCM-256 algorithm is incorrect. PR1336834
- Circuits using QSFP28-100GBASE-LR4 might find that a link does not recover after going down. Light levels will fluctuate across lanes and PCS errors will increase. Additionally, **Rx loss of signal alarm** will be active despite acceptable Rx levels. PR1337327
- First packet pertaining to Jflow Packet Forwarding Engine sensor in UDP mode is missing after line card reboot on MX150 platform. PR1344755
- When community_action is specified with community_name in NETCONF for the "insert after" operation a **parse error in identifier attributes** error is seen and insertion fails. PR1348082

- On a Next Generation Routing-Engine (NG-RE), a failure of the (Hardware Random Number Generator (HWRNG) will leave the system in a state where not enough entropy is available to operate.PR1349373
- In some cases, OIR (removal followed by reinsertion) of a MIC on a FPC can lead to silently dropped traffic that is destined to the FPC. The only way to recover from this is to restart the FPC. As a workaround, to avoid this issue, use the corresponding CLI commands to turn the MIC offline and then online. PR1350103
- Packet loop is detected when a VRF multipath is enabled with the **equal-external-internal** command under an L3VPN instance and install-nexthop is enabled in the forwarding-table export policy regarding that L3vpn route.PR1348175
- In Junos OS Release, stale access-internal routes corresponding to BOUND interfaces(clients) might remain in rpd when AIU temporarily fails before succeeding eventually. PR1350401
- When ephemeral DB instance is configured, if committing changes which are unrelated to IGMP/MLD (such as “set interfaces ge-0/0/1.0 description"), and the number of ephemeral commits reaches to ephemeral DB maximum size, the ephemeral DB purge might happen. Then it would purge all the commits and rollover. On this purge the mgd gives all the applications a FULL COMMIT view. And on this FULL COMMIT view IGMP/MLD deletes all configurations and adds it back again. This might cause PIM to prune the groups on those interfaces and send join messages again. Finally, the multicast traffic flapping and drop might be seen. PR1352499
- VRRP MAC filter will not be seen in the Packet Forwarding Engine if aggregated Ethernet interfaces flap followed by GRES occurs, that is, before VRRP state settles down after flap. During this time VRRP state was backup in the master Routing Engine and idle in the backup Routing Engine. PR1353583
- Rpd memory leak is observed for RT_NEXTHOPS_TEMPLATE. PR1357897
- On enabling hidden **command set chassis power-off-ports-on-no-master-re**, MPC7E cards can crash during switchover with two or more iteration, which is inconsistent. PR1358451
- Some of the exported packets for sessions sensor could get fragmented due to this at times the collector receives only the telemetry header part and not the payload. PR1364288
- During FPC or SFB online, if training failure is seen on a line card for 3 or more number of planes (24 planes convention), then that particular line card might not get linerate traffic (around 7-8% traffic loss). PR1365668
- A traffic drop might be seen with swap out of a VC of QFX5100 to the MX10003 for testing some heavy multicast even when IRB comes up. PR1369099

Infrastructure

- A file system corruption might create a kernel core file. The Routing Engine reboots with the message **ffs_blkfree: freeing free block**. PR1028972
- Junos OS might hang trying to acquire the SMP IPI lock while rebooting when it is running as a VM on Linux and QEMU hypervisor. PR1359339

Interfaces and Chassis

- Junos OS now checks logical interface (IFL) information under the aggregated Ethernet (AE) interface and prints the information only if it is part of it. PR1114110
- Junos OS upgrade involving Releases 14.2R5 (and later in 14.2 maintenance releases) and 16.1 (above mainline releases) with CFM configuration can cause cfmd crash after upgrade. This is due to the old version of **/var/db/cfm.db**. PR1281073
- LAG member links running LACP in slow mode might get disassociated from the LAG bundle with a combination of restart interface-control and FPC offline/online trigger. The issue was seen with scale configuration on DUT. The scale details are 2800 CFM sessions, 2800 BFD sessions, 2043 BGP peers, and 3400 VRF instances. PR1298985
- In a subscriber management scenario with dynamic demultiplexing (DEMUX) interfaces configured, in the case where subscribers belonging to one aggregated Ethernet (AE) interface are migrated to a new configured AE interface, subscribers might fail to access the device after deleting the old AE configuration. PR1322678
- CFM session does not come up if configured a logical interface (IFL) with a VLAN ID that matches the configured native VLAN ID under the physical interface (IFD).PR1325190
- When eth-oam is deactivated with scale PM configuration (under hardware-assited-pm-mode), the FPC might become unstable and generate core files. PR1347250

Layer 2 Features

- The issue occurs in routers equipped with following line cards: T4000-FPC5-3D, MX-MPC3E-3D, MPC5E-40G10G, MPC5EQ-40G10G, MPC6E, and MX2K-MPC6E. If the router is working as a VPLS PE device, due to MAC aging every 5 minutes, the VPLS unicast traffic is flooded as unknown unicast every 5 minutes. PR1148971

MPLS

- When using **mpls traffic-engineering bgp-igp-both-ribs** with LDP and RSVP both enabled, CSPF for interdomain RSVP LSPs cannot find the exit area border router (ABR) when there are two or more such ABRs. This causes interdomain RSVP LSPs to break. RSVP LSPs within the same area are not affected. As a workaround, you can either run only RSVP on OSPF ABR or IS-IS L1/L2 routers and switch RSVP off on other OSPF area 0/IS-IS L2 routers, or avoid LDP completely and use only RSVP. PR1048560
- The issue occurs when graceful Routing Engine switchover (GRES) is done between the master and backup Routing Engines of different memory capabilities. For example, one Routing Engine has only enough memory to run routing protocol process (rpd) in 32-bit mode while the other is capable of 64-bit mode. The situation could be caused by using Junos OS Release 13.3 or later with the configuration statement **auto-64-bit** configured, or by using Junos OS Release 15.1 or later even without the

configuration statement. Under these conditions, the rpd might crash on the new master Routing Engine. As a workaround, this issue can be avoided by using the CLI command **set system processes routing force-32-bit**. PR1141728

- In CE-CE setup, traffic loss might be observed over the secondary LSP on primary failover. PR1240892
- With nonstop active routing (NSR), when a routing protocol process (rpd) restarts on the master Routing Engine, rpd might also restart on the backup Routing Engine. PR1282369
- With dynamic tunnels configured, the rpd might crash when the rpd is restarted or Routing Engine switchover is executed. PR1319386
- Packets loss might be observed when auto-bandwidth is enabled for circuit cross-connect (CCC) connections and label-switched-path (LSP) no-self-ping with **no-install-to-address** is configured. PR1328129
- The LSP configuration was not able to update its admin-group when the global admin-group (under MPLS) was changed. Hence LSP was not coming up. PR1348208

Network Management and Monitoring

- A vulnerability in Junos OS SNMP MIB-II subagent daemon (mib2d) might allow a remote-network-based attacker to cause the mib2d process to crash, resulting in a denial of service condition (DoS) for the SNMP subsystem. PR1241134
- The jnxDcuStatsEntry and jnxScuStatsEntry OIDs are missing after interface configuration change. PR1354060

Platform and Infrastructure

- When using the **show | compare** method to commit, part of the configuration might be treated as noise and return a syntax error. PR1042512
- In configurations with IRB interfaces, during times of interface deletion (for example, FPC reboot), the Packet Forwarding Engine might log errors stating **nh_ucast_change:291Referenced l2ifl not found**. This condition should be transient, with the system reconverging on the expected state. PR1054798
- This issue occurs when 120 bridge domains (among a total of 1000 bridge domains) have XE/GE links toward the downstream switch and LAG bundles as uplinks toward upstream routers. The XE/GE link is part of the physical loop in the topology. Spanning-tree protocols such as VSTP/RSTP/MSTP are used for loop avoidance. Some MAC addresses are not learned on DUT when LAG bundles that are part of such bridge domains are flapped, and other events such as spanning-tree root bridge change occur. PR1275544
- DCD microbfd logs, which are debugging logs and do not indicate an error condition are seen. When micro BFD is configured they give debugging info regarding the local address configuration and commit checks. The issue here is that these logs are being populated even if micro BFDis not configured. This

PR should add a check in the Junos OS code, to make sure that these logs are not populated unless micro BFD is configured on the aggregated Ethernet (AE) interface. PR1300796

- An inaccuracy issue occurs with three-color policer of both types- single rate and two rate for certain policer rate and burst-size combination. This issue is present beginning with Junos OS Release 11.4 on platforms that use the Trio. PR1307882
- MPC5 - inline-ka PPP echo requests are not transmitted when anchor-point is lt-x/2/x or lt-x/3/x in pseudowire deployment PR1345727
- There is no support of interface range for channelized interfaces on MX10003. User has to configure interfaces individually. PR1350635
- When a tunnel interface is used as the anchor port in pseudowire services, deleting the **set interface** configuration results in the tunnel services interface being deleted. Deleting pseudo services alone will not have an effect on tunnel services interfaces. PR1350733
- Flowtap DTCP filter is not getting added due to an authorization issue. This issue happens only if a remote username and remote password configured on a remote server are used by flowtap . This issue will not happen if flowtap uses a local username and local password configured on the Junos OS device. For a remote username and remote password, the issue can be avoided per the workaround provided. This issue impacts only flowtap and has no impact on remote users logging into the device through ssh, telnet, or any utility. PR1365515

Routing Protocols

- The static/static access routes pointing to an unnumbered interface are getting added in the routing table even if the interface is down. In this case, if graceful Routing Engine switchover (GRES) is disabled, this type of route will never be added in the routing table after Routing Engine switchover. PR1064331
- JTASK_SCHED_SLIP for rpd might be seen on doing **restart routing** or **ospf protocol disable** with scaled BGP routes in the MX104 router. PR1203979
- LDP OSPF are 'in sync' state because "IGP interface down" with ldp-synchronization enabled for OSPF. . As per the current analysis, "IGP interface down" is observed as the reason because although LDP notified OSPF that LDP sync was achieved, OSPF was not able to take note of the LDP synchronization notification, because the OSPF neighbor was not up yet. PR1256434
- BGP peer flap is seen when Routing Engine switchover is triggered from the old backup Routing Engine. This issue is seen only with higher scales. The issue is related to slow draining out of the new Backup socket. PR1325804
- When **clear validation database** was issued back to back multiple times, it resulted in partial validation database (some validation of the entries were missing). This eventually recovered after up to 30 minutes (half of the record lifetime) when periodic full updates were done. PR1326256
- The issue occurs when configuring anycast and prefix segments in SPRING for IS-IS. The prefix-segment index 0 is not supported, even though user is allowed to configure 0 as an index. PR1340091

- Starting with Junos OS Release 16.1R1, there might be a mismatch in the length of the BGP update message between the BGP main thread and I/O thread when receiving BGP updates. An rpd crash might be seen. PR1341336
- In a scenario where an application allocates and caches next-hop templates, the NH template cache grows continuously. But when application clears the local cache, then memory is freed to the NH template cache. However, the NH template cache does not have code to shrink the cache and free the memory back. Hence the NH template memory is trapped in the cache and cannot be used for other purposes. But if same BGP routes and next hops come up again, they will reuse the templates from the cache and not consume additional memory. PR1346984

SEE ALSO

New and Changed Features | **87**

Changes in Behavior and Syntax | **108**

Known Behavior | **113**

Resolved Issues | **126**

Documentation Updates | **145**

Migration, Upgrade, and Downgrade Instructions | **145**

Product Compatibility | **152**

Resolved Issues

IN THIS SECTION

This section lists the issues fixed in the Junos OS Release 18.2R1 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 (ALGs)

- IKEv2 negotiation might fail with IKE ESP ALG enabled in an IKEv2 redirection scenario. PR1329611

Class of Service (CoS)

- CoS wildcard configuration is applied incorrectly after router restart. PR1325708
- The Routing Engine might get into amnesiac mode after restarting if **excess-bandwidth-share** is configured. PR1348698

EVPN

- EVPN traffic mapping to specific LSPs is not working. PR1281415
- FPC might crash if VPLS configuration is deleted. PR1324830
- Core link flap might result in an inconsistent global MAC count. PR1328956
- On deactivated ESI for packet-switched services at the physical interface (IFD) level, rpd generated a core file for EVPN-VPWS pseudowire head-end termination (PWHT). PR1332652

- On doing **restart routing**, rpd core files were generated on a provider edge (PE) router that had an EVPN-VXLAN configuration. PR1333331
- The rpd process might crash when executing CLI command **show route evpn-ethernet-tag-id**.PR1337506
- In an EVPN-VXLAN environment, BFD flaps cause VTEP flaps and cause Packet Forwarding Engine crash. PR1339084
- Traffic loss might be observed in EVPN VPWS scenario if the remote PE's interface comes down. PR1339217
- The IRB logical interface (IFL) is brought up, even if L2 interfaces are absent but IM next hops present. PR1340723
- The rpd might crash if the IRB interface and routing instance are deleted together in the same commit. PR1345519
- Traffic might be lost on Layer 2 and Layer 3 spine node in multihome EVPN scenario. PR1355165
- EVPN IRB configured with **no-gratuitous-arp-request** is still sending gratuitous ARP. PR1356360

Forwarding and Sampling

- Observing pfed core file in **pfed_process_session_state_notification_msg, pfed_timer_manager_c::remove_serv_id,pfed_delete_timer_id_by_serv_sid (serv_sid=0, serv_info=0x0) at ../../../../../../src/junos/usr.sbin/pfed/pfed_timer.cc:16** .PR1296969
- The FPC CPU might reach 100 percent constantly if shared bandwidth policer is configured. PR1320349
- Error messages about dfw_gencfg_handler might be seen during unified ISSU. PR1323795
- Some firewall filter counters might not be created in SNMP. PR1335828
- The error logical interface under VPLS might be blocked after MAC moving if the logical interfaces are on the same physical interface. PR1335880
- Commit failed when attempting to delete any demux0 unit numbers that are greater or equal to 1000,000,000. PR1348587
- With MPLS EVPN with RSVP and class-of-service-based forwarding, remote MAC is not added in the forwarding table, causing traffic to be dropped. PR1353555

General Routing

- In timing hybrid mode MX MPC2 cards are not working with ACX with vlan (native-vlan-id). PR1076666
- An rpd memory leak caused by repeated RSVP reservation state block deletes RSVP paths. PR1115686
- No warning is raised when the bridge family is configured with interface-mode trunk but without **vlan-tagging** or **flexible-vlan-tagging**. PR1154024

- Unexpected MobileNext Gateway Activation license alarm is raised when TDF gateway is configured. PR1162518
- SNMP trap sent for **PEM Input failure** alarm is not generated when single input feed fails on MX960 routers.PR1189641
- The replacement PIC might bounce when PIC PB-4OC3-4OC12-SON-SFP (4x OC-12-3 SFP) is replaced with PB-4OC3-1OC12-SON2-SFP (4x OC-3 1x OC-12 SFP) and a CLI commit is made. PR1190569
- The **Pred Fail** Fan Tray chassis alarm is renamed to **Predicted Fail**. PR1202724
- CMIC:CMIC(0/1): **Unable to deregister sub error (131072) for error(0x1b0001) for module MIC** error messages are seen on MPC5E card. PR1221337
- The error log **cc_mic_irq_status: CC_MIC(5/2) irq_status(0x1d) does not match irq_mask(0x20), enable(0x20), latch(0x1d)** is seen continuously for MIC-3D-4OC3OC12-1OC48. PR1231084
- **chassisd[9132]: LIBJSNMP_NS_LOG_NOTICE: NOTICE: netsnmp_ipc_client_connection: unix connection error: socket(-1) main_session(0x9812f80)** error messages are seen after chassis-control restart. PR1243364
- GNF sometimes resets its MPC type 9 at NSR at high scale. PR1259910
- On a vMX router, the FPC might restart unexpectedly with the message **panic (format_string=format_string@entry=0x9e509c4Thread %s attempted to %s with irq priority at %d\n**). PR1263117
- The **show chassis FPC** command does not show temperature. PR1263315
- Aggregated Ethernet incorrect counters related to PR 1261207: Incorrect counters are seen for output packets on child links for ae0 interface when configured for revertive mode. PR1273983
- For inline J-Flow, when **template-refresh-rate** and **option-referesh-rate** are configured with both packets and seconds interval options, the packets interval option is not working. PR1274206
- Software changes were provided in order to fix PR1204589 and PR1256073 that addresses the following:

  PR 1204589 - When traceroute occurs over MPLS and when the TTL expired traffic has to be generated and sent back to the source through the routing-instance, the ACX chooses the highest IP address in the routing-instance as the source, which makes it looks like the the tracepath is not correct. This behavior is modified to select the correct source address by looking into the destination routing instance and the IP address. This feature was disabled by default which has been fixed through PR1256073.

  PR1256073 - The above feature was disabled by default which is enabled with the fix of this PR. A CLI command **set system allow-6vpe-traceroute-src-select** in operational mode. PR1279191
- At commit, BSYS might log messages reporting that GNF-owned PICS do not support power-off configuration when no such configuration is present. PR1281604
- On MX Series routers with MPC7E/MPC8E/MPC9E, the threshold of corrected single-bit errors should be enhanced from 32 to 1024 and the alarm severity should changed from Major to Minor. PR1285315

- During PPPoE subscriber login, errors such as **[vbf_flow_src_lookup_enabled]** and **[failed to find iff structure, ifl]** were seen on the FPC. PR1294710
- When the system exceeds the chassis temperature limit, the log message incorrectly indicates shutdown time as 240 seconds. PR1298414
- Error messages about PEM might be seen in MX Series routers with AC PEM. PR1299284
- A chassisd core file is seen after insertion of REMX2K-X8-64 in MX2000 line routers with the older RE-S-1800x4. PR1300083
- Internal latency is high during initial subscription of sensors. PR1303393
- The mgd might crash when the Ephemeral database is used. PR1305424
- The **start shell pfe network fpc** command is not working on MX960. PR1306236
- FPC syslog errors with **pfeman_inline_ka_steering_gencfg_handler: nh not found** could mean that steering rules are not installed correctly. PR1308884
- Subscribers might not be able to access the device if dynamic VLAN is used. PR1309770
- Ninety percent of subscribers might go down after unified ISSU from Junos OS Release 16.1 to Release 17.3. PR1309983
- Utilization of **commit check** just after setting the master password can trigger improper decoding of configuration secrets. PR1310764
- The incorrect error number might be reported for syslog messages with the prefix of **%DAEMON-3-RPD_KRT_Q_RETRIES**. PR1310812
- Chassis alarm should be switched-off PEMS. PR1311574
- MX Series Virtual Chassis: BNG: IPv6 RS (router-solicit) packets are dropped in the non-default RI. This issue does not occur for the default RI. PR1313722
- The L2TP LAC might drop packets that have incorrect payload length while sending packets to the LNS. PR1315009
- The **show version detail** command gives the severity log message **mobiled: main Neither BNG LIC nor JMOBILE package is present,exit mobiled**.PR1315430
- Sensors belonging to the same producer with identical reporting intervals are not streamed in parallel. PR1315517
- The **show subscribers summary port** command does not display the correct output when subscribers are connected over pseudowire. PR1315659
- Traffic load balancing: Traffic statistics counters are not getting updated in the Junos OS Release 18.1. PR1317077
- The output from **show configuration <> | display json** might not be properly enclosed in double quotation marks. PR1317223
- Linux-based micro-kernel might panic due to concurrent update on mutable objects. PR1317961

- Adding/deleting the new Traffic Load Balancer (TLB) instance might affect other existing TLB instances. PR1318184
- CoA shaping rate is not applied successfully after unified ISSU from Junos OS Release 15.1R6.7 to Release 16.1R6.2. PR1318319
- The **show subscriber summary** displays incorrect terminated subscriber count. PR1320717
- The bbe-smgd daemon might crash after performing GRES. PR1318528
- The MPC with specific failure hardware might impact other MPCs in the same chassis. PR1319560
- Kernel core file could be seen if the number of routing instances exceeds 256. PR1319781
- Chassis MIB SNMP OIDs for VC-B member chassis are not available after MX Series Virtual Chassis unified ISSU. PR1320370
- PPP inline keepalive does not work as expected when CPE aborts the subscriber session. PR1320880
- MX Series routers send the IPv6 router advertisements and the DHCPv6 advertisements before sending IPCPv6 ACK from CPE. PR1321064
- On MX Series Virtual Chassis, CoS is not applied to the Packet Forwarding Engine when a VCP link is added. PR1321184
- While running SNMP walk and with continuous server flaps for over 1 hour, for a few instances the VS summary shows as down but RS shows as up. PR1321318
- SNMP MIB walk of TLB MIB jnxTLBMIB (gives total 27,201 lines of MIB entries) for 2 TLB instances (with a total of 17 virtual services and 730 real servers) takes around 9 minutes to complete. PR1321613
- The rpd might crash when two next hops are installed with the same next-hop index. PR1322535
- The rpd might crash when the OpenConfig package is upgraded with JTI streaming data in the background. PR1322553
- MS-MIC interface logical interfaces (IFLs) remain down after many iterations of going offline and online. PR1322854
- NCP Conf-Ack/Conf-Req packets might be dropped constantly from MLPPP client on next generation broadband subscriber management . PR1323265
- The CLI commands in **show system subscriber-management route routing-instance <XXX>** hierarchy show unexpected outputs. PR1323279
- The CLI command **request vmhost halt routing-engine other** does not halt the backup Routing Engine. PR1323546
- Subscribers might fail to log in after the interface is deactivated or activated. PR1324446
- The memory leakage is seen in mosquitto-nossl daemon. PR1324531
- SNMP interface filter does not work when **interface-mib** is part of the dynamic profile. PR1324573
- SNMP values might not be increased monolithically. PR1325128

- MPC cards might drop traffic under high temperature. PR1325271
- Ping might stop working and traffic will be dropped on the channelized port if MACsec is configured on one channel. PR1325282
- IS-IS adjacency fails to establish because of packets drop on Packet Forwarding Engine. PR1325311
- MACsec session might fail to establish on MX10003 platform. PR1325331
- The VLAN demux interface does not respond to the ARP request in a subscriber scenario with MX Series routers running Junos OS Release 15.1 or later with subscriber-management enabled. PR1326450
- MACsec MKA periodic transmit interval upper limit needs to be increased. PR1326526
- On MX Series, BNG CoS service object is not deleted properly for TCP and scheduler. PR1326853
- Some of show commands were issued twice when request support information is executed. PR1327165
- Minor alarm **LCM Peer Connection un-stable** is observed on MX150 after the chassisd process starts up or restart. PR1328119
- The following message is constantly logged: **fm_feacap_sys_feature_get:Attribute DB init not yet done, reading from pvid (id: 18)** . PR1328868
- **show class-of-service interface demux0 <demux interface> Adjustment overhead-accounting mode** do not provide the expected output. PR1329212
- When an AMS bundle has a single MAM added to it, the subinterfaces do not recover after the subinterface has been disabled. PR1329498
- Host-outbound traffic is not rewriting IEEE-802.1p bits for dynamic subscriber logical Interface (IFL) Over PS interface. PR1329555
- SNMP walks for Interfaces-related MIB objects are slower than expected in a scaled configuration. PR1329931
- The **show services nat mappings address-pooling-paired** command times out and fails. PR1330207
- The alarm **Too many supplies missing in Lower/Upper zone** flaps (set/clear) every 20 seconds if a zone does not have the minimum required PSMs. PR1330720
- In a subscriber scenario, if the BGP session is created by means of the subscriber interface, then the traffic destined to the BGP advertised prefix will be dropped. PR1330737
- Rpd core files are generated on the new backup Routing Engine at **task_quit,task_terminate_timer_callback,task_timer_dispatch,task_scheduler** after disabling NSR+GRES. PR1330750
- FPC wedge with fragmented packets occurs on LSQ interface - PT1: Head and tail out of sync. PR1330998
- A highly scaled GNF might fail to complete NSR replication after a NSR switchover. PR1331145
- Non-NEBS compliant optics might be disabled when chassis temperature exceeds non-nebs-optics-overheat-trigger. PR1331186

- The bbe-smgd process might crash after executing the command **clear ancp access-loop circuit-id <circuit id of interface set>**. PR1332096
- Inaccurate J-Flow records might be seen for the output interface and next hop. PR1332666
- On MX150 platform, **set chassis alarm management-ethernet link-down ignore** is not ignoring the alarm for FPC Mgt 0 interface. PR1332799
- Upgrading from Junos OS Release 17.3 or Release 17.4 to Junos OS Release 18.1R1 is only possible with **no-validate** command on MX10003/MX204. PR1332884
- The subinfo process might crash, and it might cause the PPPoE subscribers to get disconnected. PR1333265
- rtsblob -x prints the incorrect key. PR1333985
- AA EVPN-VXLAN causes high CPU usage on the backup rpd. PR1334235
- Two subscribers cannot reach the online state at the same time if they have an identical Frame-Route attribute value. PR1334311
- The 260G MPC with HQoS supported on Atlas (MX) went for a "restart" after unified ISSU to Junos OS Release 18.2DCB in MX2010 box. PR1334612
- MPC8E or MPC9E reports high temperature alarms and fan speed changing continuously through full and normal speed iterations. PR1334750
- The rpd crashes when performing the BGP configuration change. PR1334846
- The UID limit is reached in large-scale subscriber scenario. PR1334886
- When **show subscribers** is used and the FPC number has two digits, the interface and IPv6 address get connected together for DHCPv6 PD. PR1334904
- IPsec SA cfg name mismatch and cfg could not be pushed to the PIC. PR1334966
- Traffic drops on the MX Series LNS because of a software error or unknown family exception when traffic is destined to or coming from the MLPPP subscriber if the **routing-services** command is present in the dynamic profile used by this subscriber. PR1335276
- The master LED glows on the master and backup RCBs, while performing image upgrade on the master with GRES/NSR enabled. PR1335514
- There are hitless keychain rollover feature limitations on the MIC-MACSEC-MRATE. PR1335644
- The RIP route updates might be partially dropped when NSR is enabled. PR1335646
- The **MAC_STUCK**message might be seen on MS-MPC or MS-MIC. PR1335956
- JET application might not be respawned after a normal exit. PR1336107
- Subscriber might experience an SDB down event and drop the clients' connections when issuing **show subscribers** commands. PR1336388

- On an MX2000 with an SFB card installed, a high amount of traffic volume on MPC7E, MPC8E, or MPC9E might cause traffic drops with cell underflow messages. PR1336446
- The bbe-smgd daemon might generate core files when doing CoS configuration of logical interfaces or interface sets. PR1336852
- Configuring **lldp neighbour-port-info-display port-id** does not take effect. PR1336946
- AI-script does not get auto re-install upon a Junos upgrade on NG-Routing Engine. PR1337028
- Error log message **sdb_db_interface_remove: del ifl:si-<index> with licnese cnt non zero on** can be seen on LTS during subscriber logout. PR1337000
- FPC temperature mismatch for MPC6/8/9 occurs on MX2000 line platform. PR1339077
- DDoS counters for OSPF might not increase. PR1339364
- IPsec VPN, Session and Serviceset sensor prototype files are being added to the Junos Telemetry Interface packaging. PR1339883
- The MX10003 MPC offline button is not effective. PR1340264
- CLI shows CB states as being online after you press the RCB offline button for more than 4 seconds. PR1340431
- VRRP is stuck in the master Routing Engine during upgrade or cold boot. PR1341044
- There might be traffic loss on some subscriber sessions when more than 32,000 L2TP subscriber sessions are anchored in ASI interface. PR1341659
- The reboot of Routing Engine might occur if PPPoE interface is configured over an aggregated Ethernet or RETH interface. PR1341968
- With discard Interfaces (configured with IGMPv3), KRT queue gets stuck while deleting multicast next hop (MCNH) with error **EPERM -- Jtree walk in progress**.PR1342032
- jnxContentsType does not display details related to fixed ports and normal TIC. PR1342285
- SNMP walk might failed for LLDP related OIDs. PR1342741
- The vFPC might become absent, resulting in the total loss of traffic. PR1343170
- In an MPLS/RSVP environment, LSP might get stuck in down state with **Record route: <self> ...incomplete**.PR1343289
- Queue counters are not getting displayed in the interface details for MX150 platform once the system reboots. PR1343306
- Errors in unified ISSU because of ffp process when an upgrade from Junos OS Release 18.1 to 18.2R1 image is performed. PR1343542
- MPC7 card crashes and generates core files with DHCPv6 on static VLAN logout. PR1343965
- MX is sending IPv6 RA and the DHCPv6 advertisements before IPCPv6 Ack from CPE. PR1344472

- The ancpd process generated core files at **src/junos/usr.sbin/ancpd/ancpd_smgd.c:2299** in clearing ANCP subscribers in a scaled scenario. PR1344805
- l2cpd generates c core file (**l2cpd_ifbd_attach (ifbd=0x98914c0, vlan_id=1, line_vid=1**) after disabling mc-ae on QFX10002-60c {default vlan-scenario}, which is getting hit where Delete is missed by l2cpd because it uses sync socket read when it starts. PR1344983
- The Framed-route "0.0.0.0/0" will not be installed in MX Series platform with Junos enhanced subscriber management releases. PR1344988
- EVPN-VXLAN: ARP packet uses VRRP/virtual-gateway MAC in Ethernet header instead of IRB MAC address. PR1344990
- Rpd crash might be seen if the **no-propagate-ttl** command is set in a routing instance that has a specific route. PR1345477
- MAC address of multiple interfaces are found to be duplicate. PR1345882
- Routing Engine model changed from JNP10003-RE1 to RE-S-1600x8. PR1346054
- New PPPoE users might fail to log in. PR1346226
- **AC system error** counter in **show pppoe statistics** is not working. PR1346231
- VCCP-ADJDOWN detection is delayed on VC-Bm when deleting one VCP link on VC-Mm. PR1346328
- The twice-napt-44 sessions are not syncing to the backup SDG with stateful sync configured. PR1347086
- IPv6 MAC resolve will fail if the DHCPv6 client uses a non-EUI64 link-local address. PR1347173
- The prerequisite of installing 32-bit libstdc++ package on host is no longer needed. PR1347921
- MIC-3D-20GE-SFP-E crashed and generated core files due to ISR 2 MIC error interrupt hogging. PR1348107
- Packet loop is detected when VRF multipath is enabled with the **equal-external-internal** command under the L3VPN instance and **install-nexthop** is enabled in the forwarding-table export policy regarding that L3VPN route. PR1348175
- Unable to set fti as output for port-mirroring instance. PR1348317
- Get-config for hidden choices is not working with ODL controller. PR1348503
- Chassisd memory leak issue occurs on MX10003 and MX204 platforms and causes eventual Routing Engine switchover and crash. PR1348753
- DHCPv6 Solicit dropped on L2TP LNS in MX Series Virtual Chassis when incoming interface is on VC-master and both anchor si- interface and VCP port on VC-backup on MPC2 NG or MPC2 NG. PR1348846
- Major alarm: **Major PEM 0 Input Failure** might be observed for DC PEM. PR1349179
- MGD crashed and generated core files due to issue in nsindb infra. PR1349288

- The MTU value for subscriber's interface might be programmed incorrectly if the command **routing-services** or **protocol pim** is configured in the dynamic profile. PR1350535
- The subinfo process might crash when executing **show subscribers address <> extensive** for a DHCPv6 address. PR1350883
- The VCP port might not come back up after it is removed and added again. PR1350845
- The pfed process is consuming 80-90 percent of CPU when running subscriber management on PPC-based routers. PR1351203
- Dynamic physical interface (IFD) creation fails when the SFP optic is plugged in MX150. PR1351387
- High CPU usage of bbe-smgd process might be seen when L2BSA subscribers get stuck. PR1351696
- After GRES, the BGP neighbors at Master Routing Engine might reset and the BGP neighbors at Backup Routing Engine take long time to establish. PR1351705
- Junos Node Slicing MSE After reinstall, one JDM server complains that the pull configuration failed and falls back to the push configuration method. PR1352503
- Bbe-smgd daemon might restart in a subscriber environment. PR1352546
- On node-sliced MX Series routers, show chassis fpc errors will not appear. PR1352705
- Offlining the MIC6-100G-CFP2 MIC using CLI command might trigger FPC card crash. PR1352921
- Rpd permanently hogging CPU due to Logical System configuration commit. PR1353548
- “3D 40x 1GE(LAN) RJ45" MIC is not recognized on MX104. PR1353632
- Syslog error: **dfw_bbe_filter_bind:1125 BBE Filter bind type 0x84 index 167806251 returned 1**. PR1354435
- Aggregated Ethernet operational state goes up even though some of the member interfaces configured under the Aggregated Ethernet are down. PR1354686
- Memory leak is found in agentd. PR1354922
- The fabric chip failure alarms are observed in GRES scenario. PR1355463
- flex-flow-sizing is not working on MX204. PR1356072
- Rpd crash was seen when issuing CLI command **show dynamic-tunnels database terse** when the system has RSVP tunnels configured. PR1356254
- I2c messages from PEM/PSM are reported if SNMP is enabled. PR1356259

High Availability (HA) and Resiliency

- The ksyncd process might crash continuously on the new backup Routing Engine after performing GRES. PR1329276

- When GRES is configured in a large-scale configuration, ksyncd crashes because of replication errors and results in insufficient available space on the hard disk. PR1332791

Infrastructure

- Cleanup at thread exit causes memory leaks. PR1328273
- The fxp0 interface not accepting IP address with **master-only** applied. PR1341325
- Junos OS is no longer going to db prompt at **~ + ctl-b**. PR1352217

Interfaces and Chassis

- IPv6 neighborship is not created on IRB interface. PR1198482
- RL-dropped packets are not displayed by **show interfaces <ifl or interface-set ifl> detail/extensive** commands. PR1249164
- L2TP subscribers might not be cleared if the access-internal routes fail to install. PR1298160
- MPC CPU usage might reach 100 percent when an OTN UFEC command is configured. PR1311154
- No route exists to the address from the directly connected route. PR1318282
- Unexpected log messages might be seen if a BGP session flaps in a dynamic-tunnels GRE scenario. PR1326983
- Unexpected log messages might be seen on a router for subscriber management. PR1328251
- Traffic loss might be seen after deleting aggregated Ethernet bundle unit 1. PR1329294
- The cfmd process crashes and generates core files.PR1329779
- The interface might not work properly after FPC restarts. PR1329896
- The dcd process might crash due to memory leak and cause commit failure. PR1331185
- The transportd process might crash when you do an SNMP query on jnxoptIfOChSinkCurrentExtTable with an unsupported interface index. PR1335438
- MX Series routers might occasionally drop the first LCP configure request packet when operating in a PPPoE subscriber management configuration. PR1338516
- When in **hardware-assited-pm-mode** and pm configuration is scale, deactivate **eth-oam** can lead to FPC crash. PR1347250
- Spontaneous jpppd generated core files on the backup Routing Engine in longevity test at **../../../../../../src/junos/usr.sbin/jpppd/pppMain.cc:400**. PR1350563

- The FPC might be stuck at 100 percent for a long time when MC-AE with enhanced-convergence is configured with large-scale IFLs. PR1353397
- FPC core files related to cfmman were observed. PR1358192

Layer 2 Ethernet Services

- MX platforms might display false positive CB alarm **PMBus Device Fail**. PR1298612
- The **on-demand-address-allocation** under **dual-stack-group** does not work for IPv6. PR1327681
- The snmpget for OID dot3adInterfaceName might not work. PR1329725
- Memory leak might happen in l2cpd if the L2-learning process is disabled. PR1336720
- DHCP client is not able to connect if VLAN was modified on the aggregated Ethernet (AE) interface associated with the IRB. PR1347115
- DHCP relay agent will discard DHCP request message silently if the requested IP address has been allocated to the other client. PR1353471
- Restarting the FPC that hosts the micro BFD link might cause lacp to crash and generate core files. PR1353597

Layer 2 Features

- An rpd process memory leak is observed upon any changes in VPLS configuration, such as deleting or re-adding VPLS interfaces. PR1335914
- VPLS instance stays in NP state after LDP session flaps. PR1354784
- RE kernel might crash when OSPFv3 is configured with IPsec key authentication over IRB interface. PR1357430

MPLS

- FPC sockets disconnects and various scheduling slips occur when executing the **show ldp traffic-statistics** command with many ECMP links and L3VPN routes. PR1214961
- The rpd might crash in LDP L2circuit scenario. PR1275766
- The **show rsvp version** command cannot display **Route Session-Id Count:** field irrespective of whether session-id is present or not. PR1285756
- Traffic drop is observed during NSR switchover for RSVP P2MP provider tunnels used by MVPN. PR1293014
- The traffic in P2MP tunnel might be lost when next-generation MVPN uses RSVP-TE. PR1299580
- The output of **show mpls container-lsp** is delayed.PR1314960

- The IPv4/IPv6 multicast traffic might get dropped in MX Series Virtual Chassis when the traffic comes in through l2circuit and goes out through aggregated Ethernet (AE) member interface across Virtual Chassis members. PR1320742
- The rpd might crash when LDP p2mp recursive is configured. PR1321626
- SNMP OID counters for mplsLspInfoAggrOctets show constant value for some LSPs even though traffic is constantly increasing in **show mpls lsp statistics** output.PR1327350
- Local repair took about 150ms > expected 100ms PR1327988
- The rpd might crash on backup Routing Engine due to memory exhaustion. PR1328974
- Fate-sharing group cost no set back to default value after CLI change, removing explicit cost configuration. PR1330161
- LDP label is generated for serial interface subnet route unexpectedly. PR1346541
- The rpd crash might happen in RSVP setup-protection scenario. PR1349036
- In a very rare scenario, rpd might crash when LDP failed to allocate self-id for the P2MP FEC. PR1349224

Network Management and Monitoring

- SNMP stops or becomes very slow after a very long period of time. PR1328455
- With **interface-mib**; MX Series router is responding with **type : NoSuchInstance** for OIDs when multiple OIDs are polled in one SNMPGET request. PR1329749
- The **show pfe statistics traffic** command output will show traffic statistics as 0 for a brief time after doing "test panic" on non-traffic-carrying line card. PR1349517
- EVENTD fails to start up with syslog configuration. PR1353364

Platform and Infrastructure

- Commit-batch is thrashing, and is not restarted. PR1284271
- DCD microbfd seems to be failing in dcd_commit_check log file even when BFD is not configured. PR1300796
- MX204 performance is degraded when using firewall filter with sampling action. PR1303529
- The source MACs might leak (or not learn) between different VPLS instances at the receiving-end VPLS PE devices. PR1306293
- VPLS instance fails to learn MAC addresses upon pseudowire switchover. PR1316459
- Rate-limit configured with small temporal buffer size might cause packet loss. PR1317385
- GNF FPC hangs at unified ISSU reboot during unified ISSU. PR1318394

- The MAC might not be learnt on MX Series routers with Trio-based card due to the negative value of the bridge MAC table limit counter. PR1327723
- The packet might get dropped in LSR if MPLS pseudowire payload does not have control word and its destination MAC starts with “4”. PR1327724
- Traffic loss might be observed on LT interface PR1328371
- The tcpdump filter might not work in egress direction on ps and lt logical interfaces (IFLs).. PR1329665
- Router hits db prompt at **netisr_process_workstream_proto**. PR1332153
- RPM MIB pingResultsMinRtt, pingResultsMaxRtt, pingResultsAverageRtt response as "1" while target address is unreachable, where it should be "0". PR1333320
- Traffic loss might be seen for some flows due to network churn. PR1335302
- Commit might fail with error reading from commit script handler: error: commit script failure. PR1335349
- The MPC might crash after setting **max-queues** to a very large number. PR1338845
- Route corruption occurs in Packet Forwarding Engine with CFM enabled on aggregated Ethernet (AE). PR1338854
- Configuring the same DHCP server in different routing instances is not supported in DHCP relay scenario. PR1342019
- Commit error occurs on configuring the same **vlan-id** on different logical interfaces (IFLs) of the same lt physical interfaces (IFDs) when **ethernet-bridge** encapsulation is configured. PR1342229
- Route corruption in Packet Forwarding Engine with connectivity-fault-management enabled for L2CKT. PR1342881
- The IPv4 GPRS traffic over aggregated Ethernet (AE) interface might be dropped if gtp-tunnel-endpoint-identifier is configured. PR1347435
- EVPN-VXLAN: MX Series : Output policing action does not work on irb interfaces for VNIs. PR1348089
- FPC CPU utilization with LT interfaces is continuously at 100 percent . PR1348840
- Running RSI via the console might cause system crash and reboot. PR1349332
- ICMP error messages are not generated if 'don't fragment' packets exceed the MTU of the multiservice interface. PR1349503
- Some commands of **system ddos-protection protocols unclassified** are missing on MX2020 in Junos OS Release 17.2X75. PR1349782
- When viewing IPv6 addresses, **display rfc5952** does not work when combined with **display set**. PR1349949
- Chassisd" memory leak is seen. PR1353111
- Kernel crash occurs because the initialization of logical interface (IFL) MAC filter function is missing for Packet Forwarding Engine extended port devices. PR1353498

- The FPC would crash due to the memory leak caused by the VTEP traffic. PR1356279
- Traffic is silently dropped and the following message is seen: **JPRDS_NH:jprds_nh_alloc(),651: JNH[0] failed to grab new region for NH** messages. PR1357707

Routing Policy and Firewall Filters

- Access-internal route might fail to be leaked between routing instances when "from instance" is configured in the policy. PR1339689
- TPI-50840 vrf-target auto-derived internal policy is not cleaned up even after deleting the configuration, causing rpd core files.PR1357724

Routing Protocols

- The **show bgp summary** results are incorrect while assisting GR. PR1045151
- BGP extended communities with sub-type 4 are erroneously displayed at LINK_BANDWIDTH. PR1216696
- Rpd generates core files in the ASBR when BGP is deactivated in the ASBR before all stale labels have been cleaned up. PR1233893
- BGP MIBv2 enterprise MIB objects for InetAddress types not properly generate OIDs. PR1265504
- After bfdd restart seen an with next-generation MVPN and l2vpn route exchange occurs, causing MVPN and VPLS traffic drop. PR1278153
- Routing loops might be seen after configuring BGP Prefix Independent-Convergence (BGP PIC). PR1282520
- AA few adj-sid details are not updated in IS-IS database with lan + adjset scenario. PR1288331
- The lmpd will crash repeatedly when logical-system is configured on the same device. PR1294166
- MSDP sessions might flap when NSR/GRES is enabled. PR1298609
- While the device is booting up with a Junos OS 17.4R1 image, the following benign message is seen: **error: channel 0: chan_shutdown_read: shutdown() failed for fd 10 [i0 o3]: Socket is not connected during the image boot up with 17.4DCB** . PR1300409
- BGP traceoption logs are still written when deactivated. PR1307690
- Rpd core files are generated in **bgp_rt_send_message at ../../../../../../../../src/junos/usr.sbin/rpd/bgp/bgp_io.c:1460**.PR1310751
- BGP route age is getting refreshed when secondary path goes down with BGP PIC enabled. PR1312538
- The rpd might crash and generate core files with distributed IGMP. PR1314679
- The rpd might constantly consume high CPU usage in BGP setup. PR1315066
- The primary path of MPLS LSP might switch to the other address. PR1316861

- The inactive route cannot be installed in multipath next hop after disabling and enabling the next-hop interface in L3VPN scenario. PR1317623
- IS-IS might choose a suboptimal path after the metric change in ECMP links. PR1319338
- Traffic might get silently dropped temporarily when BGP GR is triggered and the direct interface flaps. PR1319631
- Issue occurs with tracing of the BGP L2VPN DF election community. PR1323596
- The rpd crash is seen when deactivating static route if the next-hop interface is type P2P. PR1323601
- When prefix limit is reached, increasing maximum-prefixes does not take effect. PR1323765
- BGP peer is not established after routing engine switchover when graceful-restart and BFD are enabled.PR1324475
- The validation replication database sometimes shows much more entries than the validation database after restarting the RPKI cache server. PR1325037
- The rpd process might crash continuously on both Routing Engines when **backup-spf-options remote-backup-calculation** is configured in IS-IS protocol. PR1326899
- Multiple next hops might not be installed for IBGP multipath route after IGP route update. PR1327904
- With BGP/LDP/IS-IS configurations, deleted IS-IS routes might still be visible in RIB. PR1329013
- The rpd might crash on backup Routing Engine after BGP peer is deleted. PR1329932
- Manual GRES with MX Series Virtual Chassis results in some packet loss on core facing interfaces. PR1329986
- The conditional route policy cannot withdraw all routes in BGP add-path scenario. PR1331615
- LDP route in inet.3 is missing when both OSPF rLFA and LFA protections are available and rejected by backup selection policy. PR1333198
- With introduction of PR1282672, discard next hop being installed when primary LSPinterface drops. When primary interface returns, discard next hop remains until BGP LU neighbor is cleared. This only impacts the cloned route (S=0). PR1333570
- Junos OS Release 15.1 onwards, IGMP joins are not processed with **passive allow-receive** configured on IGMP interface. PR1334913
- BGP sessions get stuck in active state after remote end (Cisco) restart the device. PR1335319
- Rpd core file is seen during delete and restore of BGP configuration. PR1338567
- The rpd crash might occur when receiving BGP updates. PR1341336
- Changes are required for displayed value of AIGP in **show route ... extensive** command. PR1342139
- Traffic might be silently dropped if the local device is receiving BFD-down. PR1342328
- The rpd might crash when BGP flaps. PR1342481
- The rpd might crash if a route for RPF uses a qualified-next-hop. PR1348550

- The rpd might crash while restarting routing or deactivating IS-IS. PR1348607
- Rpd might crash when BGP route damping and BGP multipath feature are configured. PR1350941
- Source community is not appended to RP (display issue in **show route** detail output) PR1353210

Services Applications

- PCP mappings cannot be manually cleared when a NAT pool is shared between PCP and standard NAT. PR1284261
- AVP 145 is not present in IRQ when ANCP DSL-type = 0. PR1313093
- SNMP MIBs are not yielding data related to sp- interfaces. PR1318339
- L2TP LTS might drop the first "CHAP Success" packet from LNS due to the delayed programming of /136 route on Packet Forwarding Engine. PR1325528
- The jl2tpd might crash if the RADIUS server returns 32 tunnel-server-endpoints. PR1328792
- Not all CSURQ messages are replied to if the number of sessions addressed in CSURQ is more than 107.PR1330150
- Crash occurs at **../src/junos/lib/libjuniper/mgmt-sock/mgmt_sock_select_info.c:35**. PR1337406
- The bbe-smgd process might crash if there are 65,535 L2TP sessions in a single L2TP tunnel. PR1346715
- Session limit per tunnel on LAC does not work as excepted. PR1348589
- While performing an SNMP walk on the IKE SAs that are getting deleted, IPsec tunnels might go down and an infinite loop scenario might be seen. PR1348797
- UDP checksum inserted by MS-DPC after NAT64 is not valid when incoming IPv4 packet has UDP checksum set to 0. PR1350375
- The **show services stateful-firewall flows counter** shows high numbers. PR1351295
- Jl2tpd process might crash shortly after one of L2TP destinations becomes unavailable. PR1352716
- L2TP tunnel-switch clients in subscriber session database reference the wrong routing-instance. PR1355396

Software Installation and Upgrade

- New versions of Junos OS do not have the tool for accessing aux port - /usr/libexec/interposer. PR1329843

Subscriber Access Management

- IP addresses are assigned discontinuously from the linked IP pools. PR1323829
- MX204 did not send **Radius Accounting-Off** message. PR1327822
- Multiple-radius-servers with different dynamic-request-port are not supported. PR1330802
- Subscriber might get stuck in terminated state when JSRC sync state is stuck in **FULL-SYNC in progress**. PR1337729
- In dual stack subscribers scenario with NDRA pool configured, the linked pools are not used when the first NDRA pool is exhausted. PR1351765

User Interface and Configuration

- CLI session might end abruptly while issuing the command **show configuration | compare rollback 1**.PR1331716

VPNs

- The rpd might crash after unified ISSU in a large-scale scenario with PIM configuration. PR1322530
- Moving MC-LAG from LDP-based pseudowire to BGP-based pseudowire might cause rpd crash. PR1325867
- The multicast might be rejected when PE devices running Junos OS received C-Mcast route from other vendors' PE devices. PR1327439
- MVPN sender-site configuration is not allowed with S-PMSI. PR1328052
- Rpd crashes and generates core files on backup Routing Engine with next-generation MVPN and NSR configuration. PR1328246
- Rpd crashes after committing interface-related parameters (for example, MTU change, VRF RD/RT, QoS) on PS interface with vlan-ccc encapsulation and no vlan-id. PR1329880
- Rpd might continuously crash on the backup Routing Engine and some protocols might flap on the master Routing Engine if hot-standby is configured for l2circuit or VPLS backup neighbor. PR1340474
- The rpd might crash on the backup Routing Engine when changing the l2circuit virtual-circuit-id in an NSR scenario. PR1345949

SEE ALSO

New and Changed Features | 87
Changes in Behavior and Syntax | 108
Known Behavior | 113
Known Issues | 117
Documentation Updates | 145
Migration, Upgrade, and Downgrade Instructions | 145
Product Compatibility | 152

Documentation Updates

There are no errata or changes in Junos OS Release 18.2R1 documentation for MX Series.

SEE ALSO

New and Changed Features | 87
Changes in Behavior and Syntax | 108
Known Behavior | 113
Known Issues | 117
Resolved Issues | 126
Migration, Upgrade, and Downgrade Instructions | 145
Product Compatibility | 152

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Starting in Junos OS Release 18.2R1, 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 18.2

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

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

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

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

Procedure to Upgrade to FreeBSD 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-x86-32-18.2R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-64-18.2R1.9-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-x86-32-18.2R1.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-64-18.2R1.9-limited.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

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

NOTE: After you install a Junos OS Release 18.2 **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-18.2R1.9-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-18.2R1.9-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 18.2 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

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 18.2

To downgrade from Release 18.2 to another supported release, follow the procedure for upgrading, but replace the 18.2 jinstall package with one that corresponds to the appropriate release.

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

For more information, see the Installation and Upgrade Guide.

SEE ALSO

Product Compatibility

IN THIS SECTION

Hardware Compatibility

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

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

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

Hardware Compatibility Tool

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

SEE ALSO

Junos OS Release Notes for NFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 18.2R1 for the NFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

This section describes the new features or enhancements to existing features in Junos OS Release 18.2R1 for NFX Series devices.

Hardware

- **ADSL2, ADSL2+ and VDSL2 SFP modules**—Starting in Junos OS Release 18.2R1, NFX Series devices support ADSL2, ADSL2+ and VDSL2 SFP modules. The ADSL2, ADSL2+ and VDSL2 SFP modules are supported on the SFP and SFP+ ports on the NFX150 devices. Note that the ADSL2, ADSL2+ and VDSL2 SFPs are not supported on the extension modules.

  [See ADSL2 and ADSL2+ SFP Interfaces on NFX Devices]

  [See VDSL2 Interfaces on NFX150 Devices]

Advanced Policy-Based Routing (APBR)

- **Advanced policy-based routing** —Starting in Junos OS Release 18.2R1, NFX Series devices support advanced policy-based routing (APBR), also known as application-based routing. APBR involves classifying the traffic based on the attributes of the applications and then applying filters based on these attributes to redirect the traffic. A Deep Packet Inspection (DPI) engine is used to inspect the traffic session to identify the application. APBR provides more flexible traffic-handling capabilities by offering granular control for forwarding packets based on application attributes.

  [See Advanced Policy-Based Routing on NFX Devices]

Security

- **Security**—Starting in Junos OS Release 18.2R1, NFX Series devices support the Layer 7 security features such as AppSecure (Application Tracking, Application QoS, Application Firewall), IPS, UserFW, and UTM.

  [See UTM User Guide for NFX Devices]

Virtual Network Functions

- **Support for vMX VNF on NFX250-S1 and NFX250-S2**—Starting in Junos OS Release 18.2R1, vMX can be configured as a VNF on NFX250-S1 and NFX250-S2 devices. You can use the JDM CLI to configure the vMX VNF.

  [See JDM User Guide for NFX250 Network Services Platform]

SEE ALSO

Changes in Behavior and Syntax | 156

Known Behavior | 157

Known Issues | 157

Changes in Behavior and Syntax

IN THIS SECTION

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 18.2R1 for the NFX Series.

High Availability (HA) and Resiliency

- **commit fast-synchronize** option not supported for products with single Routing Engine (NFX Series)—Starting in Junos OS Release 18.2R1, Junos OS does not support the configuration option **commit fast-synchronize** at the **[edit system]** hierarchy level for all the products with a single Routing Engine for which **chassis redundancy graceful-switchover** is not supported. This option is disabled from the CLI.

SEE ALSO

Known Behavior

IN THIS SECTION

This section lists the known limitations in hardware and software in Junos OS Release 18.2R1 for the NFX Series.

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

Allocation of hugepages

- On NFX150 running Junos OS Release 18.2R1, 700 MB of hugepages are allocated by default for use by the system components. A portion of the 700 MB is used and the remaining free memory is available for the system as well as third-party VNFs. PR1354027

SEE ALSO

New and Changed Features | 154

Changes in Behavior and Syntax | 156

Known Issues | 157

Resolved Issues | 158

Documentation Updates | 159

Migration, Upgrade, and Downgrade Instructions | 160

Product Compatibility | 162

Known Issues

IN THIS SECTION

This section lists the known issues in hardware and software in Junos OS Release 18.2R1 for the NFX Series.

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

BIOS Upgrade

- On NFX150 running Junos OS Release 18.2R1, AMI does not support ME region upgrade support using ESRT upgrade method. Hence, with latest BIOS ABDN_U_POR3-SFP_11.37.00, BIOS upgrade for ME region is not supported. PR1333875

SEE ALSO

- New and Changed Features | **154**
- Changes in Behavior and Syntax | **156**
- Known Behavior | **157**
- Resolved Issues | **158**
- Documentation Updates | **159**
- Migration, Upgrade, and Downgrade Instructions | **160**
- Product Compatibility | **162**

Resolved Issues

IN THIS SECTION

- Resolved Issues: 18.2R1 | **159**

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

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

Resolved Issues: 18.2R1

Junos Control Plane (NFX150)

- On NFX150 devices running Junos OS Release 18.2, the **file-copy** operation by a user with no super-user permissions might fail.PR1333995

SEE ALSO

New and Changed Features | **154**

Changes in Behavior and Syntax | **156**

Known Behavior | **157**

Known Issues | **157**

Documentation Updates | **159**

Migration, Upgrade, and Downgrade Instructions | **160**

Product Compatibility | **162**

Documentation Updates

There are no errata or changes in Junos OS Release 18.2R1 documentation for the NFX Series.

SEE ALSO

New and Changed Features | **154**

Changes in Behavior and Syntax | **156**

Known Behavior | **157**

Known Issues | **157**

Resolved Issues | **158**

Migration, Upgrade, and Downgrade Instructions | **160**

Product Compatibility | **162**

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.

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 18.2

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

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

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

To download and install Junos OS Release 18.2R1:

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

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

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

3. Select the **Software** tab.

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

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

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

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

10. Install the new package on the device.

SEE ALSO

Product Compatibility

IN THIS SECTION

Hardware Compatibility

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

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

Find Feature Explorer at: https://pathfinder.juniper.net/feature-explorer/.

Hardware Compatibility Tool

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

Software Version Compatibility

This section lists the vSRX and Cloud CPE Solution software releases that are compatible with the Junos OS releases on the NFX150 and NFX250 platforms:

NFX150 Software Version Compatibility

This section lists the vSRX software releases that are compatible with the Junos OS releases on the NFX150 platform:

Table 1: Software Compatibility Details with only vSRX Installed

NFX150 Junos OS Release	vSRX
18.1R1	18.1R1
18.1R2	18.1R2
18.1R3	18.1R3
18.2R1	18.2R1

NFX250 Software Version Compatibility

This section lists the vSRX and Cloud CPE Solution software releases that are compatible with the Junos OS releases on the NFX250 platform:

Table 2: Software Compatibility Details with vSRX and Cloud CPE Solution

NFX250 Junos OS Release	vSRX	Cloud CPE Solution
15.1X53-D40.3	15.1X49-D40.6	Cloud CPE Solution 2.0
15.1X53-D41.6	15.1X49-D61	Cloud CPE Solution 2.1
15.1X53-D102.2	15.1X49-D61	Cloud CPE Solution 3.0
15.1X53-D47.4	15.1X49-D100.6	Cloud CPE Solution 3.0.1
15.1X53-D490	15.1X49-D143	Cloud CPE Solution 4.0
15.1X53-D495	15.1X49-D160	Cloud CPE Solution 4.1

Table 3: Software Compatibility Details with only vSRX Installed

NFX250 Junos OS Release	vSRX
15.1X53-D40.3	15.1X49-D40.6
15.1X53-D41.6	15.1X49-D40.6
15.1X53-D45.3	15.1X49-D61

Table 3: Software Compatibility Details with only vSRX Installed *(continued)*

NFX250 Junos OS Release	vSRX
15.1X53-D47.4	15.1X49-D78.3
17.2R1	15.1X49-D75
17.3R1	15.1X49-D100
15.1X53-D471	15.1X49-D143
18.1R1	18.1R1
18.1R2	18.1R2
18.1R3	18.1R3
18.2R1	18.2R1

SEE ALSO

- New and Changed Features | **154**
- Changes in Behavior and Syntax | **156**
- Known Behavior | **157**
- Known Issues | **157**
- Resolved Issues | **158**
- Documentation Updates | **159**
- Migration, Upgrade, and Downgrade Instructions | **160**

Junos OS Release Notes for PTX Series Packet Transport Routers

IN THIS SECTION

These release notes accompany Junos OS Release 18.2R1 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

This section describes the new features and enhancements to existing features in Junos OS Release 18.2R1 for the PTX Series.

Hardware

- **Next-generation fixed configuration packet transport router (PTX Series)**— Starting in Junos OS Release 18.2R1, the new PTX10002-60C features a compact, 2 U form factor that is easy to deploy in space-constrained Internet exchange locations, remote central offices, and embedded peering points throughout the network, including cloud-hosted services. The PTX10002-60C has 60 QSFP28 transceiver ports that you can configure as 100 Gbps, 40 Gbps, or 4 by 10 Gbps. The ports handle up to 6 Tbps of throughput and 4 Bpps of forwarding capacity. The PTX10002-60C is available with either AC or DC power supplies, and it has airflow out, where air comes into the vents in the port panel and exhausts through the field-replaceable unit (FRU) panel.
- **PTX10K-LC1105 MACsec line card on PTX10008 and PTX10016 routers**—Starting in Junos OS Release 18.2R1, PTX10K-LC1105 line card provides 30 ports of either 100-gigabit or 40-gigabit QSFP28 with MACsec features.

  [See PTX10000 Line Card Components and Descriptions.]

Class of Service (CoS)

- **Support for class of service (CoS) on PTX10002-60C routers**—Starting in Junos OS Release 18.2R1, PTX10002-60C routers support CoS.

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

  [See Understanding CoS CLI Configuration Statements on PTX Series Routers.]

High Availability (HA) and Resiliency

- **Resiliency Support for PTX10008 and PTX10016 routers with JNP10K-RE1**—Starting with Junos OS Release 18.2R1, resiliency support is enabled for PTX10008 and PTX10016 routers with the JNP10K-RE1 Routing and Control Boards.

Interfaces and Chassis

- **Support for PTX10K-LC1105 line card (PTX10008)**—Starting with Junos OS Release 18.2R1, PTX10008 routers support the PTX10K-LC1105 line card. The line card is designed to provide secure Ethernet communication across high-speed links. The card consists of 30 QSFP+ or QSFP28 Pluggable ports that are Media Access Control Security (MACsec) capable. The ports support speeds of 100 Gbps or 40 Gbps, which can be configured using the CLI.
- **Protection against distributed denial-of-service (DDoS) attacks (PTX10002-60C)**—Starting in Junos OS Release 18.2R1, PTX10002-60C devices support DDoS protection for many Layer 2 and Layer 3 protocol families and packet types. DDoS attacks typically use network control packets to trigger a large number of exceptions in the network, consuming resources and crippling network operations. DDoS protection uses firewall filters and policers available in Junos OS to discard or rate-limit control plane traffic so that malicious traffic does not overwhelm and bring down a device. To configure DDoS protection, use the **ddos-protection** statement at the **[edit system]** hierarchy level to specify the desired protocol groups, control packet types, and filter parameters.

  [See Understanding Distributed Denial-of-Service Protection on PTX Series and QFX Series Devices.]

- **Channelization support (PTX Series)**—Starting with Junos OS Release 18.2R1, you can use channelization functionality to subdivide a larger flexible optical interface into subinterfaces or channels. PTX Series routers have 12 ASIC circuits (PE) as a part of a Packet Forwarding Engine, and each PE switch has 5 ports (one standalone MAC port and 4 channelized MAC ports). The standalone MAC ports cannot be channelized. On the router, you can channelize 48 ports out of the available 60 ports.

  By default, the ports come up in a mode that does not support channelization.

  To enable channelization on an interface:

```
[edit chassis fpc fpc-slot pic pic-slot]
user@switch# set port port-number speed speed
```

[See Channelizing Interfaces.]

Junos Telemetry Interface

- **Streaming OpenConfig data from Routing Engine sensors over UDP in protobuf format (MX Series, PTX Series, QFX Series)**–Starting in Junos OS Release 18.2R1, you can stream OpenConfig-based sensor data from Routing Engine sensors using the Junos Telemetry Interface (JTI). This allows you to stream the OpenConfig sensor data in gRPC/protobuf format rather than in key/value pairs. This makes the messages smaller and is more efficient.

  [See Overview of the Junos Telemetry Interface.]

- **Routing Engine state sensors for the Junos Telemetry Interface (MX Series, PTX Series)**—Starting with Junos OS Release 18.2R1, you can export statistics for the Routing Engine state through the Junos Telemetry Interface using the following resource paths:

  - **/junos/kernel-ifstate/stats/churn-rate**
  - **/junos/kernel-ifstate/stats/peer-consumption-rate**
  - **/junos/kernel-ifstate/stats/vetos-statistics**

  Only gRPC streaming is supported.

  To provision the sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module.

  Support for the Junos Telemetry Interface was introduced on QFX10000 and QFX5200 switches in Junos OS Release 17.2R1.

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

- **Expanded ON_CHANGE support for Junos Telemetry Interface (JTI) (MX Series, PTX Series)**—Starting with Junos OS Release 18.2R1, OpenConfig support through remote procedure call (RPC) and JTI is extended to support additional ON_CHANGE sensors.

  Periodical streaming of OpenConfig operational states and counters collects information at regular intervals. ON_CHANGE support streams operational states as events (only when there is a change), and is preferred over periodic streaming for time-sensitive missions.

  These paths, previously supporting periodical streaming only, now also support ON_CHANGE streaming:

  - **/interfaces/interface/state/admin-status**
  - **/interfaces/interface/state/description**

- **/interfaces/interface/state/oper-status**
- **/interfaces/interface/subinterfaces/subinterface/state/admin-status**
- **/interfaces/interface/subinterfaces/subinterface/state/description**
- **/interfaces/interface/subinterfaces/subinterface/state/oper-status**
- **/interfaces/interface/subinterfaces/subinterface/state/ifIndex**
- **/interfaces/interface/subinterfaces/subinterface/state/index**
- **/interfaces/interface/subinterfaces/subinterface/state/name**

These resource paths from the preceding list do not change with an event, but will be streamed on creation and deletion:

- **/interfaces/interface/subinterfaces/subinterface/state/ifIndex**
- **/interfaces/interface/subinterfaces/subinterface/state/index**
- **/interfaces/interface/subinterfaces/subinterface/state/name**

To provision a sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires you to download the OpenConfig for Junos OS module.

To enable ON_CHANGE support, configure the sample frequency in the subscription as zero. When you create a subscription using a top-level container as the resource path (for example, **/interface**), leaf devices under the resource path **/interface** with ON_CHANGE support are automatically streamed based on events. Other leaf devices will not be streamed.

Before events are streamed, there is an initial stream of states to the collector, followed by an **END_OF_INITIAL_SYNC**. This notice signals the start of event streaming.

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

- **J-Insight Device Monitor (PTX Series)**–J-Insight is a data-driven device monitoring solution that provides visibility and insight into the health of a running system. Starting with Junos OS Release 18.2R1, the J-Insight framework facilitates real-time monitoring of system resources for FPC FRUs. It also has been integrated with the existing connectivity error management infrastructure to normalize error detection, monitoring, and reporting. J-Insight is an on-premise system application that uses the Junos Telemetry Interface to continuously collect data that is reflective of the current state and health of the device component being monitored.

  [See J-Insight Device Monitor Overview.]

Layer 3 Features

- **Support for Layer 3 unicast features on PTX10002-60C**—Starting in Junos OS Release 18.2R1, PTX10002-60C routers support the following Layer 3 features for unicast IPv4 and IPv6 traffic:

- OSPF
- IS-IS
- BGP

MPLS

- **LDP support (PTX10002-60C)**—Starting in Junos OS Release 18.2R1, the PTX10002-60C router supports the Label Distribution Protocol (LDP). LDP is a protocol for distributing labels in non-traffic-engineered applications. LDP enables routers to establish label-switched paths (LSPs) through a network by mapping network-layer routing information directly to data link layer-switched paths. [See MPLS Applications User Guide for Routing Devices.]
- **RSVP support (PTX10002-60C)**—Starting in Junos OS Release 18.2R1, the PTX10002-60C router supports RSVP. RSVP is a resource reservation setup protocol that is used by both network hosts and routers. Hosts use RSVP to request a specific class of service (CoS) from the network for particular application flows. Routers use RSVP to deliver CoS requests to all routers along the datapath. RSVP can also maintain and refresh states for a requested CoS application flow. [See MPLS Applications User Guide for Routing Devices.]
- **MPLS capabilities (PTX10002-60C)**—Starting in Junos OS Release 18.2R1, MPLS capabilities are available on the PTX10002-60C router. MPLS provides both label edge router (LER) and label-switching router (LSR) capabilities, and supports the following features:
  - Object access method, including ping, traceroute, and Bidirectional Forwarding Detection (BFD)
  - Fast reroute (FRR) which is a component of MPLS local protection. Both one-to-one local protection and many-to-one local protection are supported.
  - Loop-free alternate (LFA)
  - IPv6 Provider Edge (6PE) and IPv6 VPN Provider Edge (6VPE) devices
  - Layer 3 VPNs for both IPv4 and IPv6
  - Layer 2 circuit

  [See MPLS Applications User Guide for Routing Devices.]
- **Support for IS-IS segment routing (PTX10002-60C)**—Starting in Junos OS Release 18.2R1, IS-IS segment routing support is enabled through MPLS. Junos OS IS-IS implementation allocates node segment label blocks to support segment routing node segments. It also provides a mechanism to the network operator to provision an IPv4 or IPv6 address family node segment index. To configure segment routing (also known as source packet routing), use the following configuration statements at the **[edit protocols isis]** hierarchy level:
  - **source-packet-routing**
  - **node-segment**

  - **use-source-packet-routing**
  - **no-advertise-adjacency-segment**

  [See IS-IS User Guide.]

- **Egress peer engineering of service labels (such as BGP and MPLS) and egress peer protection for BGP-LU (PTX10002-60C)**—Starting in Junos OS Release 18.2R1, you can enable traffic engineering of service traffic, such as MPLS LSP traffic between autonomous systems (ASs), by using BGP-labeled unicast for optimum utilization of the advertised egress routes. You can specify one or more backup devices for the primary egress AS boundary router. Junos OS installs the backup path in addition to the primary path in the MPLS forwarding table, which enables MPLS fast reroute (FRR) when the primary link fails. It provides support for the FRR protection backup scheme to perform an IP lookup to determine a new egress interface.

  [See Configuring Egress Peer Traffic Engineering by Using BGP Labeled Unicast and Enabling MPLS Fast Reroute.]

- **IPv6 tunneling over an MPLS-based IPv4 network (PTX10002-60C)**—Starting in Junos OS Release 18.2R1, tunneling enables you to connect IPv6 sites over an IPv4 MPLS-enabled backbone. IPv6 packets are carried over an IPv4 MPLS tunnel. To enable this service, you need to deploy provider edge (PE) routers that can run IPv4, MPLS, and BGP toward the core and IPv6 toward the edge.

  [See Example: Tunneling IPv6 Traffic over MPLS IPv4 Networks.]

- **MPLS inter-AS link protection (PTX10002-60C)**—Starting in Junos OS Release 18.2R1, MPLS inter-AS link protection is supported. Link protection is essential in an MPLS network to ensure traffic restoration in case of an interface failure. The ingress router will then choose an alternate link through another interface to send traffic to its destination.

  For an MPLS inter-AS environment, link protection can be enabled when **labeled-unicast** is used to send traffic between autonomous systems (ASs). To configure link protection on an interface, the **protection** statement is introduced at the **[edit protocols bgp group *group-name* family inet labeled-unicast]** hierarchy level.

  [See Understanding MPLS Inter-AS Link Protection.]

Multicast

- **Support for multicast protocols (PTX10002-60C) routers**—Starting in Junos OS Release 18.2R1, PTX10002-60C routers support the following multicast protocols:

  - Protocol Independent Multicast sparse mode— PIM sparse mode enables efficient routing to multicast groups with receivers sparsely spread over multiple networks. To configure PIM sparse mode, include the **pim** statement at the **[edit protocols]** hierarchy level. PIM sparse mode supports static RP addresses, bootstrap routers, automatic RP announcement and discovery, and anycast RP functionality.

    [See Understanding PIM Sparse Mode.]

- PIM source-specific multicast (PIM SSM)— PIM source-specific multicast uses a subset of PIM sparse mode and IGMPv3 to enable a client to receive multicast traffic directly from the source. PIM source-specific multicast uses the PIM sparse-mode functionality to create a shortest-path tree (SPT) between the client and the source, but builds the SPT without the help of a rendezvous point.

  [See Understanding PIM Source-Specific Mode.]

- Internet Group Management Protocol (IGMP)—IGMP manages the membership of hosts and routing devices in multicast groups.

Network Management and Monitoring

- **sFlow functionality introduced on the PTX1000 and PTX10000 platforms**—Starting in Junos OS Release 18.2R1, the PTX1000 and PTX10000 routers support sFlow, a network monitoring protocol for high-speed networks. With sFlow, you can continuously monitor tens of thousands of ports simultaneously. The mechanism used by sFlow is simple, not resource intensive, and accurate. An sFlow agent embedded in a network device samples packets and gathers interface statistics and sends the information to a monitoring station called a *collector* for analysis. An sFlow agent can be implemented in a distributed model. In such a case, each subagent has a separate subagent ID and is responsible for monitoring a set of network ports. The subagents share a common agent address.

  [See Configuring sFlow Technology for Network Monitoring (CLI Procedure) and sflow.]

- **Support for Junos Space Service Now (PTX10008 and PTX10016)**—Starting in Junos OS Release 18.2R1, PTX10008, and PTX10016 routers support Junos Space Service Now. Junos Space Service Now is an application that runs on the Junos Space Network Management Platform to automate fault management and accelerate issue resolution.

  [See Junos Space Service Now.]

- **Support for port mirroring on PTX10002-60C routers**—Starting in Junos OS Release 18.2R1, PTX10002-60C routers supports port mirroring. Port mirroring copies packets entering or exiting a port and sends the copies to a local interface for local monitoring. You can use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on.

  [See Configuring Port Mirroring.]

Operation, Administration, and Maintenance (OAM)

- **Connectivity fault management (CFM) support (PTX Series)**—Starting with Junos OS Release 18.2R1, PTX5000 routers with FPC-P2 support Ethernet OAM CFM on the child links of tagged aggregated Ethernet bundles for IPv4 traffic, thereby enabling you to monitor faults on those child links.

  The CFM supports fault monitoring and path discovery functionalities.

  > **NOTE:** To enable CFM on an Ethernet interface, you must configure maintenance domains, maintenance associations, and maintenance association end points (MEPs).
  >
  > [See IEEE 802.1ag OAM Connectivity Fault Management Overview .]

Routing Policy and Firewall Filters

- **Support for firewall filters and policers on PTX10002-60C routers**—Starting in Junos OS Release 18.2R1, you can define firewall filters on the PTX10002-60C routers that define whether to accept or discard packets. The PTX10002-60C routers support IPv4 filters, IPv6 filters, and MPLS filters.

  You can also use policing to apply limits to traffic flow and specify the action to be taken for packets that exceed those limits.

  [See Firewall Filters Overview.]

Services Applications

- **Support for multiple flow collectors for inline flow monitoring (PTX Series)**—Starting in Junos OS Release 18.2R1, you can export flow records generated by inline flow monitoring to four collectors under a family with the same source IP address. The Packet Forwarding Engine can export the flow record, flow record template, option data, and, option data template packet to all configured collectors. You can configure the multiple collectors at the **[edit forwarding-options sampling instance instance name]** hierarchy level.

  [See Monitoring Network Traffic Flow Using Inline Flow Monitoring on PTX Series Routers.]

- **Support for inline flow monitoring (PTX10008 and PTX10016)**—Starting in Junos OS Release 18.2R1, Junos OS supports inline active flow monitoring. Inline active flow monitoring supports version 9 and IPFIX flow collection templates. Version 9 template is supported for IPv4, IPv6, and MPLS. IPFIX template is supported for IPv4, IPv6, and MPLS. Both IPFIX and version 9 templates use UDP as the transport protocol.

  [SeeMonitoring Network Traffic Flow Using Inline Flow Monitoring on PTX Series Routers.]

- **Support for MPLS, MPLS-IPv4, and MPLS-IPv6 inline active flow monitoring (PTX Series)**—Starting in Junos OS Release 18.2R1 on PTX Series routers, you can perform inline flow monitoring for MPLS,

MPLS-IPv4, and MPLS-IPv6 traffic. Both IPFIX and version 9 templates are supported. Inline flow monitoring for MPLS-over-UDP flows was supported in Junos OS Release 18.1R1.

[See Configuring Inline Active Flow Monitoring on PTX Series Routers.]

Software Installation and Upgrade

- **Zero Touch Provisioning (PTX3000, PTX5000, PTX10008, PTX10016)**—Starting in Junos OS Release 18.2R1, Zero Touch Provisioning (ZTP) is supported to automate the provisioning of the device configuration and software image with minimal manual intervention.

  When you physically connect a router to the network and boot it with a factory configuration, the router attempts to upgrade the Junos OS software image automatically and autoinstall a configuration file from the network through the management interface on PTX5000, PTX3000, PTX10008, and PTX10016 routers. The router uses information configured on a DHCP server to locate the necessary software image and configuration files on the network. If you have not configured the DHCP server to provide this information, the router boots with the pre installed software and factory-default configuration. The ZTP process either upgrades or downgrades the Junos OS version.

  [See Understanding Zero Touch Provisioning and Configuring Zero Touch Provisioning.]

- **ZTP support (PTX10002-60C switch)**—Starting with Junos OS Release 18.2R1, ZTP, automates the provisioning of the device configuration and software image with minimal manual intervention, and is supported on PTX10002-60C VM hosts. When you physically connect a supported device to the network and boot it with a factory configuration, the device attempts to upgrade the Junos OS software image automatically and autoinstall a configuration provided on the DHCP server.

  [See Zero Touch Provisioning.]

System Management

- **Support for request vmhost and show vmhost commands (PTX10002-60C switches)**—Starting in Junos OS Release 18.2R1, many of the **request system** and **show system** commands have been replaced with **request vmhost** and **show vmhost** commands.

  Here is a list of the vmhost commands that are now supported:

  - request vmhost cleanup
  - request vmhost file-copy
  - request vmhost halt
  - request vmhost hard-disk-test
  - request vmhost power-off
  - request vmhost power-on

- request vmhost reboot
- request vmhost snapshot
- request vmhost software add
- request vmhost software rollback
- request vmhost zeroize
- show vmhost bridge
- show vmhost crash
- show vmhost hard-disk-test
- show vmhost hardware
- show vmhost information
- show vmhost logs
- show vmhost management-if
- show vmhost netstat
- show vmhost processes
- show vmhost resource-usage
- show vmhost snapshot
- show vmhost status
- show vmhost uptime
- show vmhost version

[See VM Host Operations and Management for more information.]

SEE ALSO

Changes in Behavior and Syntax | 176
Known Behavior | 179
Known Issues | 182
Resolved Issues | 185
Documentation Updates | 188
Migration, Upgrade, and Downgrade Instructions | 189
Product Compatibility | 195

Changes in Behavior and Syntax

IN THIS SECTION

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 18.2R1 for the PTX Series.

High Availability (HA) and Resiliency

- **commit fast-synchronize** option not supported for products with single Routing Engine (PTX Series)—Starting in Junos OS Release 18.2R1, Junos OS does not support the configuration option **commit fast-synchronize** at the **[edit system]** hierarchy level for all the products with single Routing Engine for which **chassis redundancy graceful-switchover** is not supported. This option **commit fast-synchronize** is disabled from the CLI.

Interfaces and Chassis

- **Power supply alarm is not raised when the input switch status is OFF or power is not connected (PTX10008, PTX10016)**—Starting in Junos OS Release 18.2R1, the power supply alarm **A power supply input has failed** will not be raised if INP1/INP2 switch status if OFF and the power is not connected. In earlier releases, an alarm is raised for the Power Entry Module (PEM) that are not powered on as **Not Powered** irrespective of the switch state. Now, to know the power supply status, execute the **show chassis power** or **show chassis power detail** CLI command. The **DC input** is the new output parameter that provides information about the status of the input feed.

  Previous behavior:

  user@host> show chassis power

  ```
  PEM 0:
  ```

```
  State:     Online
  Capacity:  2500 W (maximum 2500 W)
  DC output: 864 W (zone 0, 72 A at 12 V, 34% of capacity)

PEM 1:
  State:     Online
  Capacity:  2500 W (maximum 2500 W)
  DC output: 864 W (zone 0, 72 A at 12 V, 34% of capacity)

System:
  Zone 0:
      Capacity:          7500 W (maximum 7500 W)
      Allocated power:   6525 W (975 W remaining)
      Actual usage:      2616 W
  Total system capacity: 7500 W (maximum 7500 W)
  Total remaining power: 975 W

...
```

Current behavior:

user@host> show chassis power

```

PEM 0:
  State:     Online
  Capacity:  2500 W (maximum 2500 W)
  DC input:  OK (No feed expected, Both feed connected)
  DC output: 576 W (zone 0, 48 A at 12 V, 23% of capacity)

PEM 1:
  State:     Online
  Capacity:  2500 W (maximum 2500 W)
  DC input:  OK (No feed expected, Both feed connected)
  DC output: 576 W (zone 0, 48 A at 12 V, 23% of capacity)

...
```

[See show chassis power.]

Junos OS XML API and Scripting

- **Junos XML protocol <open-configuration> operation no longer emits an uncommitted changes warning (PTX Series)**—Starting in Junos OS Release 18.2R1, the Junos XML protocol **<open-configuration>** operation does not emit an "**uncommitted changes will be discarded on exit**" warning message when opening a private copy of the candidate configuration. However, Junos OS still discards the uncommitted changes upon closing the private copy.

Junos Telemetry Interface

- **Change to the configuration location for gRPC-based sensor subscriptions from an external collector (PTX Series)**—Starting in Junos OS Release 18.2R1, when an external streaming server, or collector, provisions sensors to export data through gRPC on devices running Junos OS, the sensor configuration is committed to the **junos-analytics** instance of the ephemeral configuration database, and the configuration can be viewed by using the **show ephemeral-configuration instance junos-analytics** operational command. In earlier releases, the sensor configuration is committed to the default instance of the ephemeral configuration database.

Network Management and Monitoring

- **New context-oid option for trap-options configuration statement to distinguish the traps that come from a non-default routing instance and non-default logical system (PTX Series)**—In Junos OS Release 18.2R1, a new option, **context-oid**, for the **trap-options** statement allows you to handle prefixes such as <routing-instance name>@<trap-group> or <logical-system name>/<routing-instance name>@<trap-group> as an additional varbind.

  [See trap-options.]

Software Installation and Upgrade

- **New DHCP option introduced for ZTP retry (PTX Series)**—Starting in Junos OS Release 18.2R1, a new DHCP option is introduced to set the timeout value for the file downloads over FTP. If the **transfer-mode** is set as FTP, the default value for the timeout is automatically set as 120 minutes. That is, if the FTP session gets interrupted due to loss of connectivity in the middle of a file transfer, it will time out after 120 minutes and ZTP will attempt to retry the file-fetching process. This value can be overridden using the DHCP option as follows:

```
option NEW_OP.ftp-timeout code 7 = text;
option NEW_OP.ftp-timeout “val”;
```

where **“val”** is the user configurable timeout value in seconds and must be provided within double quotation marks (for example, "val").

SEE ALSO

- New and Changed Features | **165**
- Known Behavior | **179**
- Known Issues | **182**
- Resolved Issues | **185**
- Documentation Updates | **188**
- Migration, Upgrade, and Downgrade Instructions | **189**
- Product Compatibility | **195**

Known Behavior

IN THIS SECTION

This section contains the known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.2R1 for the PTX Series.

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

General Routing

- When an FPC goes offline or restarts, FPC 'x' sends traffic to FPC 'y'. The following error messages are seen on the destination FPC. A corresponding alarm is set on the destination FPC. Specific to PTX10000, the transient alarm gets set when this condition occurs. The alarm clears later because the source FPC goes offline. **Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Error (0x210613), module: PE Chip, type: Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Cmerror Op Set: PE Chip: PE1[1]: FO:core intr: 0x00000010: Grant spray drop due to unspray-able condition error Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Error (0x210614), module: PE Chip, type: Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Cmerror Op Set: PE Chip: PE1[1]: FO:core intr: 0x00000008: Request spray drop due to unspray-able condition error** PR1268678
- MPLS Ingress LSP statistics is not supported. PR1337814
- When unsupported sensors are configured, the sensors are subscribed to on the device, but no data is exported. PR1339559

- The Routing Engine boots from the secondary disk when you:
  - Press the reset button, on the RCB front panel, while Routing Engine is booting up but before Junos is up.
  - Upgrade software, by booting from the network using the **request vmhost reboot network** command, and the system fails to boot from the network.
  - Upgrade BIOS and the upgrade fails.
  - Reboot and the system hangs before Junos is up. PR1344342
- Due to ZH ASIC limitation, MAC statistics under show interface, in Routing Engine, may not reflect "Mac error Counters" properly if ingress packet size is greater than default mtu (1518) or user configured mtu size (set interface <interface-name> mtu <288...9600> PR1345779
- If a customer uses PXEboot, MAC address used will not be the same as runtime Junos and what must be configured in the PXE servers. PR1354113
- Ingress LSP statistics is not supported. Only transit LSP statistics are supported, and it's limited to 24,000 only. PR1355909
- 100G DAC connected between QFX5200 and PTX10002-60C/QFX10002-60C will not link up. This is because BCM based devices have link-training enabled and PE based devices do not have link-training enabled for 100G DAC/CR4. PR1356834

Infrastructure

- When L3 interface comes up, there can be mismatch in IFL counters between Routing Engine and Junos Telemetry Interface. This mismatch pertains to ARP/GARP packets. As ARP/GARP packet that gets initiated the moment L3 interface comes up(from spirent/DUT) Routing Engine ends up having one packet less on IFL. PR1361282

Interfaces and Chassis

- On PTX10008 and PTX10016 routers, if you remove the redundant Switch Interface Board (SIB) after upgrading Junos OS from Release 17.4R1 or Release 17.2X75-D90 to a later release, then an alarm is not generated. This is a known behavior and has no impact on the performance of the router.

SEE ALSO

New and Changed Features | **165**

Changes in Behavior and Syntax | **176**

Known Issues | **182**

Known Issues

IN THIS SECTION

This section lists the known issues in hardware and software in Junos OS Release 18.2R1 for the PTX Series.

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

General Routing

- When the CFP2-DCO-T-WDM-1 is plugged in the PTX Series PIC, after repeated configuration rollbacks, the link sometimes can take a long time to come up. PR1301462
- On PTX Series platforms, an error message could be observed when FPC card goes online or off line. PR1322491
- On PTX Series platforms with TQ-chip cards (for example, FPC1 or FPC2) and class of service (CoS) used, a high-priority queue might not get the entire configured bandwidth. PR1324853
- On 30-Port MACsec line card (LC1101-M - 30C / 30Q / 96X) of Vale-PTX chassis, under certain circumstances, when the **exclude-protocol lacp** configuration under the **[edit security macsec connectivity-association connectivity-association-name]** hierarchy level, is deleted or deactivated, the LACP "Mux State", shown under the output of the CLI command **show lacp interface**, might remain as "attached" or "detached" and would not transition to "distributing" state. PR1331412

- Filters configured with the scale-optimized flag pointing to traffic-class-count will not increment. PR1334580
- Some default Routing Engine sensors are subscribed as part of default j-insight package. PR1339329
- On PTX5000 routers, multicast traffic packet drop is observed. This issue occurs because of the interoperability of the of TQ-chip with PTX Series routers based line cards. PR1339481
- The same port range (0..19) is used for both PIC 0 and PIC 1. PR1342081
- On next-generation Routing Engines, a failure of the Hardware Random Number Generator (HWRNG) leaves the system in a state where not enough entropy is available to operate. PR1349373
- Host path statistics may not match between Routing Engine and Packet Forwarding Engine. PR1353699
- Traffic loss duration during FRR link-protection is in the range of 25 through 150 msec. PR1355953
- MACsec configuration on a 40-Gbps port might lead to invariable traffic drops in some scenarios. As a workaround, configure the speed over the interfaces and reboot the routers before doing the MACsec configuration. PR1357849
- Some of the test cases pertaining to restarting of Routing Engine daemons is causing a random crash of aftman-expr Packet Forwarding Engine daemon and resulting in FPC restart and breaking of GRPC connection. PR1360941
- Around 5 percent traffic loss seen when graceful_switchover done on non DUT with super core profle two configuration. **request chassis routing-engine master acquire no-confirm** command is used to do switchover on R1's standby Routing Engine. PR1363740
- With TIC offline/online, MPLS bidirectional traffic flow might stop working. PR1367920

Infrastructure

- A file system corruption might create a kernel core file. The Routing Engine reboots with the message **ffs_blkfree: freeing free block**. PR1028972
- In Junos OS Release 16.1R1 and later releases, PTX Series routers might get to abnormal state due to F-Label exhaustion. The protection mechanism for warning and protecting F-Label exhaustion malfunctions on these releases after network churn. PR1336207

Interfaces and Chassis

- Junos OS upgrades involving releases 14.2R5 (and later maintenance releases) and 16.1 (and later maintenance releases) with CFM configuration can cause cfmd crash after upgrade. This is due to the old version of **/var/db/cfm.db**. PR1281073

MPLS

- When the rpd daemon is terminating, the process of signaling the deletion of all RSVP LSPs might take so long that a watchdog timer is triggered, resulting in an rpd core file. PR1257367

Platform and Infrastructure

- Status LED on the chassis does not show up on PTX10002-60C with Junos OS 18.2R1.9 image. Juniper recommends customers to upgrade to Junos OS 18.2R1.10 image and follow up with a jfrmware upgrade with the following command:

  request vmhost system software add /volume/build/junos/18.2/release/18.2R1.10/ship/jfirmware-vmhost-x86-64-18.2R1.10.tgz

  After the jfirmware upgrade, a power cycle is mandatory for the device to be operational in normal state. PR1332991

- Execution of Python scripts through enhanced automation is only supported on non-veriexec images. PR1334425

SEE ALSO

New and Changed Features | **165**

Changes in Behavior and Syntax | **176**

Known Behavior | **179**

Resolved Issues | **185**

Documentation Updates | **188**

Migration, Upgrade, and Downgrade Instructions | **189**

Product Compatibility | **195**

Resolved Issues

IN THIS SECTION

This section lists the issues fixed in Junos OS 18.2R1 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

- Remove **show chassis spmb** command and response. PR1244059
- For MTRE devices using telemetry, **restart na-grpc-server** and **restart na-mqtt** do not work. PR1284121
- For BGP-LU multipath routes, if there is a forwarding-table export policy configured to reject such routes, then rpd might might crash during next-hop installation. PR1297044
- Interfaces might go down when the Packet Forwarding Engine encounters **TOE::FATAL ERROR**. PR1300716
- The FPC is being reported as down in chassisd logs related to streaming telemetry, eventhough the FPC is online. PR1300795
- A third-generation FPC (FPC3-SFF-PTX) might not boot on a PTX3000 with the Control Board or Routing Engine. PR1303295
- Internal latency is high during initial subscription of sensors. PR1303393
- The mgd might process crash when the Ephemeral database is used. PR1305424
- Packet Forwarding Engine error messages are flooding as **expr_sensor_update_cntr_to_sid_tree** after delete and rollback of **protocols isis source-packet-routing node-segment**. PR1309288
- Need to suppress chassis alarm for switched off PEM. PR1311574

- The SIB LED on the front panel display is green and remains steadily lit even before an SIB comes online. PR1311632
- When the user changes the PIC or port speed, an alarm is raised and user intervention is required. PR1311875
- Memory leak in the chassisd process occurs while streaming telemetry subscriptions are active. PR1315672
- Packet Forwarding Engine packet drop is seen on the PTX5000 when there is a 100-ms RTT delay between the DUT and the collector. PR1316429
- On the PTX10000, for 100G LR4 Optics with part number 740-061409, need to change **show chassis hardware** display to QSFP-100G-LR4-T2. PR1322082
- The rpd might crash when an OpenConfig package is upgraded with JTI streaming data in the background. PR1322553
- On PTX1000, MX204, MX10003, or QFX10002-60C, the local time on the FPC might be different from the local time on the Junos VM or VM host. PR1325048
- The GRE traffic is not de-encapsulated by the firewall filter. PR1325104
- Firewall filter is not supported on aggregated Ethernet. PR1325237
- PTX Series MKA sessions are not coming up after changing CA parameters such as - **transmit-interval**, and **key-server-priority**. PR1325392
- MPLS traceroute fails across PTX Series platform. PR1327609
- Unsupported features need to be removed or disabled under CLI **set vlans <vlan_name>**. PR1328219
- Unsupported options need to be disabled under CLI **set interfaces <interface_name> unit 0 family ethernet-switching interface-mode trunk**. PR1328507
- Link instability occurs after link-down event on PTX Series device. PR1330708
- Traffic stops flowing out of ae70 after some FPC restart iterations. PR1335118
- PTX5000 FPC might reboot in certain rare scenarios when interface-specific policer is configured. PR1335161
- Disabling a breakout 10G port on et-0/0/5 will unexpectedly disable another breakout 10G port on et-0/0/5. PR1337975
- FPC/FPC2/FPC E on PTX Series device does not forward traffic. PR1339524
- Link goes down on PTX3000/PTX5000 with FPC3 inserted after router reboot or link flap. PR1340612
- On the PTX1008, the 30-Port Coherent Line Card (DWDM-IC) does not come up. PR1344732
- No DHCP service or configuration is running after the system has cleared. PR1347730
- Sensors are not getting cleared up after doing Routing Engine switchover. PR1347779

- Threshold is not getting configured correctly in PTX Series device when threshold is configured using scope and category options. PR1350841
- BFD sessions do not come up on PTX3000. PR1352112
- Flabels might get exhausted after multiple Routing Engine switch-over. PR1354002
- The interface of 15 100G ports PIC might delay 60 seconds to come up. PR1357410

Infrastructure

- The ixlv interface statistics are not accounted for properly. PR1313364

Interfaces and Chassis

- On the PTX3000, failed to check CFM neighbors wrt **show oam ethernet connectivity-fault-management interfaces ae0.0 extensive**. PR1335305
- The transportd process might crash when an SNMP query is performed on jnxoptIfOChSinkCurrentExtTable with an unsupported interface index. PR1335438

MPLS

- Traffic drop is seen during NSR switchover for RSVP P2MP provider tunnels used by MVPN. PR1293014
- Traffic loss occurs for static LSP configured with the **stitch** command. PR1307938
- The rpd might crash on the backup Routing Engine due to memory exhaustion. PR1328974
- MPLS LSP statistics are not shown in cli command **show mpls lsp ingress statistics**. PR1344039

Platform and Infrastructure

- DCD Microbfd seems to be failing in dcd_commit_check log file even when BFD is not configured. PR1300796
- Traffic might be silently dropped and the following message might be seen: **JPRDS_NH:jprds_nh_alloc(),651: JNH[0] failed to grab new region for NH messages**. PR1357707
- Unable to commit junos configuration during the ZTP process and ZTP process stop completed. PR1358919

Routing Protocols

- The rpd might constantly consume high CPU resources in a BGP setup. PR1315066
- The primary path of MPLS LSP might switch to another address. PR1316861
- The rpd process might crash continuously on both Routing Engines when **backup-spf-options remote-backup-calculation** is configured in IS-IS protocol. PR1326899
- Protocol churn will create rpd crash. PR1341466

SEE ALSO

New and Changed Features | **165**

Changes in Behavior and Syntax | **176**

Known Behavior | **179**

Known Issues | **182**

Documentation Updates | **188**

Migration, Upgrade, and Downgrade Instructions | **189**

Product Compatibility | **195**

Documentation Updates

There are no errata or changes in Junos OS Release 18.2R1 documentation for the PTX Series.

SEE ALSO

New and Changed Features | **165**

Changes in Behavior and Syntax | **176**

Known Behavior | **179**

Known Issues | **182**

Resolved Issues | **185**

Migration, Upgrade, and Downgrade Instructions | **189**

Product Compatibility | **195**

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.

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 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 acting as the backup Routing Engine.

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

Basic Procedure for Upgrading to Release 18.2

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

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

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

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

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

To download and install Junos OS Release 18.2R1:

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

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

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

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

4. Select the **Software** tab.

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

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

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

> **NOTE:** After you install a Junos OS Release 18.2R1 jinstall package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the request system software add validate command and specify the jinstall package that corresponds to the previously installed software.

The validate option validates the software package against the current configuration as a prerequisite to adding the software package to ensure that the router reboots successfully. This is the default behavior when the software package being added is for a different release. Adding the **reboot** command reboots the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process might take 5 to 10 minutes. Rebooting occurs only if the upgrade is successful.

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

```
user@host> request system software add validate reboot
source/jinstall-18.2R1.SPIN-domestic-signed.tgz
```

All other customers, use the following command:

```
user@host> request system software add validate reboot
source/jinstall-18.2R1.SPIN-export-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

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

NOTE: After you install a Junos OS Release 18.2 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

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

Installing the Software on PTX10002-60C Routers

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 PTX10002-60C 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-ptx-x86-64-18.2R1.9.tgz
```

If the Install Package resides remotely from the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add
ftp://ftpserver/directory/junos-vmhost-install-ptx-x86-64-18.2R1.9.tgz
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

SEE ALSO

Product Compatibility

IN THIS SECTION

Hardware Compatibility

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

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

Hardware Compatibility Tool

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

SEE ALSO

Junos OS Release Notes for the QFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 18.2R1 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Caveat: Juniper Networks does not recommend configuring and deploying EVPN-VXLAN on QFX Series platforms running Junos OS 18.2R1.

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

New and Changed Features

IN THIS SECTION

This section describes the new features for the QFX Series switches in Junos OS Release 18.2R1.

> **NOTE:** The following QFX Series platforms are supported in Release 18.2R1: QFX5100, QFX5110, QFX5200, QFX5210, QFX10002, QFX10008, and QFX10016.

Hardware

- **QFX10000-30C-M line card supports channelization (QFX10008 and QFX10016 switches)**–Starting in Junos OS Release 18.2R1. 40-Gigabit Ethernet ports on the QFX10000-30C-M line card can be channelized to 10-Gigabit Ethernet. When ports are in channelization mode, every fifth port is disabled. [See QFX10000-30C-M Line Card .
- **Support for JNP-QSFP-100G-BXSR transceiver (QFX5200)**—Starting in Junos OS Release 18.2R1, the QFX5200 switches support the JNP-QSFP-100G-BXSR transceiver. The 100-Gbps bidirectional transceiver has a dual transmitter/receiver that allows it to transmit and receive data through a single optical fiber. Each bidirectional transceiver has two LC receptacles that receive and transmit on different optical wavelengths. The wavelength of the input optical signal needs to match the receive wavelength of the pairing transceiver. For example, if transceiver A has a transmit wavelength of 850 nm and a receive wavelength of 900 nm, then the pairing transceiver B should have a matching receive wavelength of 850 nm and a transmit wavelength of 900 nm. [See the Hardware Compatibility Tool.]

Authentication Access Control

- **Enhancement to NTP authentication method (QFX5110,QFX10000)**— Starting in Junos OS Release 18.2R1, Junos OS supports NTP authentication for both SHA-1 and SHA2-256, in addition to the existing

NTP authentication method, MD5. You can now choose from among MD5, SHA-1, and SHA2-256 for synchronizing the clocks of Juniper Network routers, switches, and other security devices on the Internet. Using SHA-1 instead of MD5 improves the security of devices with very little impact to timing, while using SHA2-256 provides an increase in security over SHA-1.

> **NOTE:** By default, network time synchronization is unauthenticated.

To implement authentication, use **set authentication-key <*key_number*> type** at the **[edit system ntp]** hierarchy level.

- To enable SHA-1 authentication, use **set authentication key <*key_number*> type sha1 value <*password*>** at the **[edit system ntp]** hierarchy level.
- To enable SHA2-256 authentication, use **set authentication key <*key_number*> type sha256 value <*password*>** at the **[edit system ntp]** hierarchy level.

[See authentication-key and Configuring NTP Authentication Keys.]

EVPN

- **Support for firewall filtering and policing on EVPN-VXLAN traffic (QFX5100, QFX5100 Virtual Chassis, and QFX5110 switches)**—Starting with Junos OS Release 18.2R1, you can configure firewall filters and policers on VXLAN traffic in an EVPN topology. Firewall filters provide rules that define whether to accept or discard packets that are transiting an interface. Policing, or rate limiting, lets you control the amount of traffic that enters the switch and further determines the actions to be taken when the traffic exceeds the defined limit. You configure firewall filters at the **[edit firewall]** hierarchy level. For each firewall filter that you apply to a VXLAN, you can specify **family ethernet-switching** to filter Layer 2 (Ethernet) packets, or **family inet** to filter on IRB interfaces. The IRB interface acts as a Layer 3 routing interface to connect the VXLANs in one-layer or two-layer IP fabric topologies. You can only apply firewall filters and policers on CE-facing interfaces in the ingress direction (traffic entering the VXLAN). For IRB interfaces, you can only apply filtering at the ingress point of non-encapsulated frames routed through the IRB interface.

  [See Understanding VXLANs and Overview of Firewall Filters.]

- **IPv6 data traffic support through an EVPN-VXLAN overlay network (QFX5110 switches)**—Starting with Junos OS Release 18.2R1, QFX5110 switches that function as Layer 3 VXLAN gateways can route IPv6 data traffic through an EVPN-VXLAN overlay network. With this feature enabled, Layer 2 or Layer 3 data packets from one IPv6 host to another IPv6 host are encapsulated with an IPv4 outer header and transported over the IPv4 underlay network. The Layer 3 VXLAN gateways in the EVPN-VXLAN overlay network learn the IPv6 routes through the exchange of EVPN Type 2 and Type 5 routes. To enable IPv6 data traffic support, you configure the IRB interfaces on all Layer 3 VXLAN gateways with the same IPv4 and IPv6 anycast virtual gateway addresses (VGAs). To support this feature, no other IPv6 configuration is required in the underlay or overlay networks.

(The feature described above is documented but not supported on QFX5110 switches in Junos OS Release 18.2R1.)

[See Routing IPv6 Data Traffic Through an EVPN-VXLAN Network with an IPv4 Underlay.]

- **Support for OSPF, IS-IS, BGP, and static routing on IRB interfaces in EVPN-VXLAN networks (QFX5110)**—Starting in Junos OS Release 18.2R1, you can configure OSPF, IS-IS, BGP, and static routing with bidirectional forwarding detection (BFD) on an IRB interface that is used as a routed interface in EVPN. This configuration allows protocol adjacencies to be established between an IRB interface on a Layer 3 gateway and a CE device and between an IRB interface on a Layer 3 gateway and a CE device connected to a Layer 2 leaf device in an EVPN-VXLAN network.

  [See Supported Protocols on an IRB Interface in EVPN-VXLAN .]

- **Support for IS-IS on IRB interfaces in EVPN-VXLAN networks (QFX 10000)**—Starting in Junos OS Release 18.2R1, you can configure IS-IS on an IRB interface that is used as a routed interface in EVPN. This configuration allows protocol adjacencies to be established between an IRB interface on a Llayer 3 gateway and a CE device and between an IRB interface on a Layer 3 gateway and a CE device connected to a Layer 2 leaf device in an EVPN-VXLAN network.

  [See Supported Protocols on an IRB Interface in EVPN-VXLAN .]

- **NOTE:** QFX5110 and QFX5200 switches do not currently support the pop functionality, which has the following implications for this feature:

  - The following use cases are not supported:
    - Traffic Pattern 1: Popping an S-VLAN tag
    - Traffic Pattern 4: Popping and later pushing an S-VLAN tag
  - Without the pop functionality, this feature does not actually support the tunneling of Q-in-Q traffic through an EVPN-VXLAN overlay network. The functionality that is currently supported is flexible VLAN tagging.

Tunneling Q-in-Q traffic through an EVPN-VXLAN overlay network (QFX5110 and QFX5200 switches)—Starting with Junos OS Release 18.2R1, QFX5110 and QFX5200 switches that function as Layer 2 VXLAN tunnel endpoints (VTEPs) can tunnel single-tagged and double-tagged Q-in-Q packets through an Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) overlay network. In addition to tunneling Q-in-Q packets, the ingress and egress VTEPs can perform the following Q-in-Q actions:

- Delete, or pop, an outer service VLAN (S-VLAN) tag from an incoming packet.
- Add, or push, an outer S-VLAN tag onto an outgoing packet.
- Map a configured range of customer VLAN (C-VLAN) IDs to an S-VLAN.

> **NOTE:** The QFX5110 and QFX5200 switches do not support the pop and push actions with a configured range of VLANs.

The ingress and egress VTEPs support the tunneling of Q-in-Q packets and the Q-in-Q actions in the context of specific traffic patterns.

[See Examples: Tunneling Q-in-Q Traffic in an EVPN-VXLAN Overlay Network.]

Junos Telemetry Interface

- **Packet Forwarding Engine sensors for the Junos Telemetry Interface (QFX5100, QFX5110, and QFX5200 Switches)** —Starting with Junos OS Release 18.2R1, you can export Packet Forwarding Engine statistics through the Junos Telemetry Interface using native sensors. Native sensors export data close to the source, such as the line card or network processing unit (NPU), using the User Datagram Protocol (UDP).

  The native sensors listed in Table 1 are supported.

  Table 4: Supported Packet Forwarding Sensors

Sensor	Exports
/junos/system/linecard/qmon-sw/ **TIP:** This sensor is only available on QFX5000 Series Switches.	Statistics for congestion and latency monitoring
/junos/system/linecard/interface/logical/usage/	Logical interface statistics
/junos/system/linecard/firewall/	Filter statistics
/junos/system/linecard/interface/	Physical interface statistics
/junos/services/label-switched-path/usage/	Label-switched paths (LSP) statistics
/junos/system/linecard/cpu/memory/	Network Processing Unit (NPU)/Line Card memory

  For streaming statistics through UDP, all parameters are configured at the **[edit services analytics]** hierarchy level.

  Support for the Junos Telemetry Interface was introduced on QFX10000 and QFX5200 switches in Junos OS Release 17.2R1.

  [See sensor and Configuring a Junos Telemetry Interface Sensor (CLI Procedure).]

- **Streaming OpenConfig data from Routing Engine sensors over UDP in protobuf format (QFX Series)**–Starting in Junos OS Release 18.2R1, you can stream OpenConfig-based sensor data from Routing Engine sensors using the Junos Telemetry Interface (JTI). This allows you to stream the OpenConfig sensor data in gRPC/protobuf format rather than in key/value pairs. This makes the messages smaller and is more efficient.

  [See Overview of the Junos Telemetry Interface.]

Port Security

- **IPv6 Router Advertisement (RA) guard (QFX5100/QFX5110/QFX5200)**—Starting with Junos OS Release 18.2R1, IPv6 RA guard is supported on QFX5100, QFX5110, and QFX5200 switches. RA guard protects networks against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. RA guard works by validating RA messages based on whether they meet certain criteria, which is configured on the switch as a policy. RA guard inspects the RA message and compares the information contained in the message attributes to the policy. Depending on the policy, RA guard either drops or forwards the RA messages that match the conditions.

  [See Understanding IPv6 Router Advertisement Guard.]

- **Client link-layer address option 79 for DHCPv6 (QFX5100/QFX5100-VC, QFX5110/QFX5110-VC, QFX5200, QFX10002, QFX10008, QFX10016)**—Starting in Junos OS Release 18.2R1, you can configure DHCPv6 option 79 to insert the DHCPv6 client link-layer address in the header of the DHCPv6 RELAY-FORWARD message that is sent from the client to the upstream device. The client link layer address can be used along with other identifiers to associate DHCPv4 and DHCPv6 messages from a dual-stack client.

  [See Inserting the DHCPv6 Client MAC Address Option (Option 79) In DHCPv6 Packets].

Restoration Procedures Failure

- **Device recovery mode introduced in Junos OS with upgraded FreeBSD (QFX Series)**—Starting in Junos OS Release 18.2R1, for devices running Junos OS with upgraded FreeBSD, provided you have saved a rescue configuration on the device, there is an automatic device recovery mode that goes into action should the system go into amnesiac mode. The new process is for the system to automatically retry to boot with the saved rescue configuration. In this circumstance, the system displays the banner **Device is in recovery mode** in the CLI (in both the operational and configuration modes). Previously, there was no automatic process to recover from amnesiac mode. A user with load and commit permission had to log in using the console and fix the issue in the configuration before the system would reboot.

  [See Saving a Rescue Configuration File.]

Routing Protocols

- **Remote LFA support for LDP in IS-IS and OSPF (QFX5100, QFX5110, QFX5200)**—Beginning with Junos OS Release 18.2R1, you can configure a remote loop-free alternate (LFA) to extend the backup provided by the LFA in an IS-IS or OSPF network. This feature is useful especially for Layer 1 metro rings where the remote LFA is not directly connected to the PLR. The existing LDP implemented for the MPLS tunnel setup can be reused for the protection of IS-IS and OSPF networks and subsequent LDP destinations thereby eliminating the need for RSVP-TE backup tunnels for backup coverage.

  To configure remote LFA over LDP tunnels in an IS-IS network, include the **remote-backup-calculation** statement at the **[edit protocols isis backup-spf-options]** hierarchy level and the **auto-targeted-session** statement at the **[edit protocols ldp]** hierarchy level.

  [See Example: Configuring Remote LFA over LDP Tunnels in IS-IS Networks. and Example: Configuring Remote LFA Over LDP Tunnels in OSPF Networks.]

Security

- **Support for CCC firewall filters (QFX10000 switches)**—Starting with Junos OS Release 18.2R1, you can configure inbound and outbound firewall filters with counter and policer actions on Layer Layer 2 circuit cross-connect (CCC) traffic (**family ccc**). This feature is beneficial if you use Layer 2 point-to-point circuits to connect customers between sites and want to use policers to apply limits to traffic flowing over CCC circuits. You configure Layer 2 firewall filters at the **[edit firewall filter family ccc]** hierarchy level.

  [See CCC Overview and Firewall Filter Match Conditions for Layer 2 CCC Traffic.]

Software Installation and Upgrade

- **Zero Touch Provisioning (QFX10008 and QFX10016 switches)**—Starting with Junos OS Release 18.2R1, you can use Zero Touch Provisioning to provision new Juniper Networks switches in your network automatically without manual intervention. When you physically connect a switch to the network and boot it with a default configuration, it attempts to upgrade the Junos OS software automatically and autoinstall a configuration file from the network. The switch uses information that you configure on a Dynamic Host Configuration Protocol (DHCP) server to locate the necessary software image and configuration files on the network

  [See Zero Touch Provisioning.]

System Management

- **Support for the Precision Time Protocol (PTP) AES67, SMPTE ST-2059-2, and AES67+SMPTE profiles (QFX5110-48S and QFX5200 switches)**—Starting in Junos OS Release 18.2R1, 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 standard allows multiple video sources to stay in synchronization across various equipment by providing time and frequency synchronization to all devices. This profile supports 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]** Junos OS CLI hierarchy.

  See [Understanding the PTP Media Profiles].

- **Zero Touch Provisioning (QFX10002-60C switches)**—Starting with Junos OS Release 18.2, Zero Touch Provisioning allows you to provision new Juniper Networks routers in your network automatically without manual intervention. When you physically connect a switch to the network and boot it with a default configuration, the switch attempts to upgrade the Junos OS software image automatically and autoinstall a configuration file from the network. The switch uses information that you configure on a Dynamic Host Configuration Protocol (DHCP) server to locate the necessary software image and configuration files on the network. If you do not configure the DHCP server to provide this information, the switch boots with the preinstalled software and default configuration. The Zero Touch Provisioning process either upgrades or downgrades the Junos OS version.

  [See Understanding Zero Touch Provisioning.]

- **New tool to detect high CPU utilization (QFX Series)**—Starting in Junos OS Release 18.2R1, a flight recorder tool is introduced to gather historical data on when the CPU utilization on a device was high and what processes caused the high utilization. The tool collects snapshots of data enabling detection of high CPU usage and faster resolution of issues.

  Because some of the high CPU utilization cases are intentional or expected, you can enable and disable the flight recorder tool to avoid false alarms.

  [See request flight-recorder set high-cpu and show flight-recorder status.]

VLAN Infrastructure

- **Flexible Ethernet support (QFX10K Switches)**—Starting in Junos OS Release 18.2R1, you can configure inet, inet6, or VLAN circuit cross connect (CCC) connections on a physical or aggregated Ethernet interface. This allows you to set different forwarding rules for tagged and untagged traffic on the same interface. For example, you can forward tagged packets over the l2circuit and route untagged traffic normally in the native VLAN mode.

  All logical devices that are under the flexible VLAN tagging are identified by their vlan-id configuration. For untagged traffic, the association to the corresponding logical device is derived using the native vlan id configuration on the physical device. For traffic without a VLAN tag, the default vlan id (native vlan id) is used to derive the layer2 domain.

SEE ALSO

Changes in Behavior and Syntax | 204

Known Behavior | 208

Known Issues | 211

Resolved Issues | 216

Documentation Updates | 223

Migration, Upgrade, and Downgrade Instructions | 223

Product Compatibility | 237

Changes in Behavior and Syntax

IN THIS SECTION

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 18.2R1 for the QFX Series.

High Availability (HA) and Resiliency

- **commit fast-synchronize** option not supported for products with single Routing Engine (QFX Series)—Starting in Junos OS Release 18.2R1, Junos OS does not support the configuration option **commit fast-synchronize** at the **[edit system]** hierarchy level for all the products with single Routing Engine for which **chassis redundancy graceful-switchover** is not supported. This option is disabled from the CLI.

Junos OS XML, API, and Scripting

- **Junos XML protocol <open-configuration> operation no longer emits an uncommitted changes warning (QFX Series)**—Starting in Junos OS Release 18.2R1, the Junos XML protocol **<open-configuration>** operation does not emit an "**uncommitted changes will be discarded on exit**" warning message when opening a private copy of the candidate configuration. However, Junos OS still discards the uncommitted changes upon closing the private copy.

Junos Telemetry Interface

- **Change to the configuration location for gRPC-based sensor subscriptions from an external collector (QFX Series)**—Starting in Junos OS Release 18.2R1, when an external streaming server, or collector, provisions sensors to export data through gRPC on devices running Junos OS, the sensor configuration is committed to the **junos-analytics** instance of the ephemeral configuration database, and the configuration can be viewed by using the **show ephemeral-configuration instance junos-analytics** operational command. In earlier releases, the sensor configuration is committed to the default instance of the ephemeral configuration database.

Network Management and Monitoring

- **New context-oid option for trap-options configuration statement to distinguish the traps which come from a non-default routing instance and non-default logical system (QFX Series)**—In Junos OS Release 18.2R1, a new option, **context-oid**, for the **trap-options** statement allows you to handle prefixes such as <routing-instance name>@<trap-group> or <logical-system name>/<routing-instance name>@<trap-group> as an additional varbind.

  [See trap-options.]

Routing Policy and Firewall Filters

- **Support for configuring the GTP-TEID field for GTP traffic (QFX5000 line of switches)**—Starting in Junos OS Release 18.2R1, the **gtp-tunnel-endpoint-identifier** statement is supported to configure the hash calculation of IPv4 or IPv6 packets that are included in the GPRS tunneling protocol–tunnel endpoint identifier (GTP-TEID) field hash calculations. The **gtp-tunnel-endpoint-identifier** configuration statement is configured at the **[edit forwarding-options enhanced-hash-key family inet]** hierarchy level.

  In most of the cases, configuring **gtp-tunnel-endpoint-identifier** statement is sufficient for enabling GTP hashing. After enabling, if GTP hashing does not work, it is recommended to capture the packets using relevant tools and identify the offset value. As per standards, 0x32 is the default header offset value. But, due to some special patterns in the header, offset may vary to say 0x30, 0x28, and so on. In this cases, use **gtp-header-offset** statement to set a proper offset value. Once the header offset value is resolved, run **gtp-tunnel-endpoint-identifier** command for enabling GTP hashing successfully.

  [See gtp-tunnel-endpoint-identifier and gtp-header-offset.]

Software Installation and Upgrade

- **New DHCP option introduced for ZTP retry (QFX Series)**—Starting in Junos OS Release 18.2R1, a new DHCP option is introduced to set the timeout value for the file downloads over FTP. If the **transfer-mode** is set as FTP, the default value for the timeout is automatically set as 120 minutes. That is, if the FTP session gets interrupted due to loss of connectivity in the middle of a file transfer, it will timeout after 120 minutes and ZTP will attempt to retry the file-fetching process. This value can be overridden using the DHCP option as follows:

```
option NEW_OP.ftp-timeout code 7 = text;
option NEW_OP.ftp-timeout “val”;
```

  where **“val”** is the user configurable timeout value in seconds and must be provided within double quotation marks(for example, "val”).

SEE ALSO

New and Changed Features | 196

Known Behavior | 208

Known Issues | 211

Resolved Issues | 216

Documentation Updates | 223

Migration, Upgrade, and Downgrade Instructions | 223

Product Compatibility | 237

Known Behavior

IN THIS SECTION

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 18.2R1 for the QFX Series.

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

General Routing

- L3 multicast traffic does not converge to 100 percentage and a few continuous drops are observed after bringing an interface down and back up again or while an FPC comes online after FPC restart. This behavior is seen when scaling beyond 2000 VLANs or 2000 IRBs with VLAN replication configured. PR1161485
- VLAN tag is removed for inter-VNI traffic on Layer 3 gateway when the encapsulation or de-encapsulation VLAN command is enabled. PR1185295
- When per-packet load balancing is removed or deleted, the next-hop index might change. PR1198092
- Single-bit and multiple-bit ECC errors are not logged on QFX5110 switches. PR1251917
- On the QFX10000-12C-DWDM coherent line card, it is possible that sometimes the link flap when MACsec is enabled on Ethernet interfaces. PR1253703
- On QFX10000 series switches, at initialization, the port group module comes up after some time and negative ACKs are seen until the port group module is up. Once the port group module is up, negative ACKs are no longer observed. This is an expected behavior due to an aggressive link scan feature introduced in Junos OS Release 17.2. PR1271579
- On QFX10000 line platforms, with a high scale of 4000 VNIs or 200,000 MACs, or both, if a large configuration change happens with traffic flowing, then forwarding descriptor memory corruption might occur, leading to complete traffic loss on certain ports. The qualification shows that a system with 400

VNIs has been stable. However, other configurations like global MAC count and underlying MPLS LSPs can increase system load. PR1296089

- Traffic drop occurs on sending traffic over "et" interfaces due to CRC errors. PR1313977
- Port LEDs on QFX5100 do not work. If a device connects to a port on QFX5100, the port LED stays unlit. PR1317750
- On a QFX10016, permanent traffic loss is seen for some hosts after the initial ARP timer expiry caused by an ARP entry is not synchronized between the two PE devices. PR1322288
- On the QFX10016 EVPN-VXLAN scaled testbed, it takes up to 3 minutes for traffic to converge when a configuration related to a tenant (5 IRBs/VLAN) is added. PR1323042
- In a MH EVPN-VXLAN scenario, with IGMP snooping configured, in a scaled scenario: 1) For 10000 s,g scale: Trigger: disable DF link for convergence: Total convergence for 10000 s,g scale is 4.5 seconds with traffic rate of 60 kpps. Per flow convergence loss ranges from 3.16 seconds to 5.66 seconds 2) For 8000 s,g scale: Trigger :disable DF link for convergence: Total convergence for 8000 s,g scale is 2.86 seconds with traffic rate of 60 kpps. Per flow convergence loss ranges from 1.86 seconds to 3.73 seconds. PR1323155
- Traffic statistics for multicast stream on GR-interfaces does not work on QFX5000 platform. PR1323622
- With 100G DAC/copper cable connected between QFX5210-64C and QFX10000 devices, links might not come up reliably. The rest of the 100G Optics/AOC, 40G Optics/DAC/Copper works well when connected between QFX5210-64C and QFX10000 devices. PR1324600
- Configuration of **mac-table-size** under VLAN switch options is not supported for QFX10002-60C. PR1325315
- In QFX5210-64C, irrespective of the physical interface speed, the speed displayed for GR-interface is always 800 mbps. PR1325695
- The **mac-learning-limit** option is not supported under VLAN switch options for QFX10002-60C platform. PR1325752
- Few harmless error messages related to function rt_mesh_group_add_check() is seen during reboot. PR1335363
- Traffic statistics does not get updated on gr-0/0/0 interface with ECMP. PR1335670
- On switching platforms, LACP aggregate Ethernet minimum-link with sync-reset enabled feature is not supported on an aggregate interface where micro BFD is enabled. PR1342657
- Hardware watchdog does not work on QFX10008 and QFX10002-60C/PTX10002-60C platforms. PR1343131
- When the routes are changed from V4 to V6 or vice versa, routes are getting added from STC before all previous routes are deleted. Hence, error messages are seen. PR1350719

EVPN

- EVPN/VXLAN implementations support up to 100 EVPN VLAN-based routing instances. Above 100 instances, MAC learning might behave incorrectly. PR1287644

Interfaces and Chassis

- As link speed configuration statement cannot be hidden and causes unexpected behavior with MC LAG peer status. PR1329030
- Supported ARP scale is 48000 over MCLAG interfaces. PR1334321

Layer 2 Features

- On QFX5100 Virtual Chassis interfaces on which flexible VLAN tagging has been enabled, STP, RSTP, MSTP, and VSTP protocols are not supported. PR1075230
- In QFX5210-64C platform, resilient hashing is not supported for LAG interfaces. PR1325499
- Packet statistics are not supported for logical child members of aggregated Ethernet (AE) interface. PR1335454

Routing Protocols

- The route unidimensional limit is 1.6 million routes in Junos OS Release 18.1R1. PR1320865
- Removal and adding of em0 configuration cause physical interface to be reconfigured. This might cause BFD to flap if aggressive BFD timers are configured due to hardware interrupt in the kernel. QFX5100 platform does not support BFD for minimum interval of less than 1 second. PR1332229

Virtual Chassis

- Virtual Chassis internal loop might happen at a node coming up from a reboot. During nonstop software upgrade (NSSU) on an QFX5100 Virtual Chassis, a minimal traffic disruption or traffic loop(>2s) might occur and it is considered to be known behavior. PR1347902

SEE ALSO

New and Changed Features | **196**

Changes in Behavior and Syntax | **204**

Known Issues | **211**

Known Issues

IN THIS SECTION

This section lists the known issues in hardware and software for the QFX Series switches in Junos OS Release 18.2R1.

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

EVPN

- The error message **JPRDS_DLT_ALPHA KHT** shows as failed, but the entries in hardware are programmed correctly. This might cause confusion regarding working and nonworking conditions. PR1258933
- On QFX10000 line switches, subinterfaces from the same physical port do not work if they are configured under the same VLAN or routing instance. An attempt to commit such a configuration fails for Layer 2 configurations but not for EVPN and VXLAN. For EVPN and VXLAN configurations, in few circumstances it would be necessary to configure a subinterface from the same physical port to support VLAN bundling. PR1278761
- In a scaled setup, if mac-move is triggered more than 4 times, the MAC move detection might not be reliable. PR1284315

- When a VLAN uses an IRB interface as the routing interface, the vlan-id parameter must be set to "none" to ensure proper traffic routing. This issue is platform independent. PR1287557
- On QFX10000, in an EVPN collapsed L2 and L3 multihomed GWs topology, when traffic is sent from IP fabric toward EVPN, some traffic loss is seen. If the number of hosts behind EVPN gateways is increased, the traffic loss becomes higher. PR1311773
- When a virtual tunnel end point (VTEP) scale of more than 200 is used in Junos OS Release 18.1R1, VTEPs might not come up for all the tunnels and might impact traffic. PR1342175
- The rpd has unreproducible generates a core file with scaling EVPN-VXLAN configuration on QFX10000 platform due to memory depletion on EVPN MAC route entries queue for L2ALD. L2ALD closed the IPC connection which caused rpd cumulated EVPN MAC route entries the in queue and ends up running out of memory. PR1339979
- On QFX5110 and QFX5200 switches that are configured to tunnel Q-in-Q traffic in an EVPN-VXLAN network, the pop operation does not work on ingress interfaces. PR1344102
- On a scaled EVPN-VxLAN setup, loading the scaled configuration and the base configuration alternately for a few times, can result in losing adjacency and hence the protocols will be down. PR1349659
- In a high scaled EVPN-VXLAN environment, when the Packet Forwarding Engine is restarted in a peer device leading to the VXLAN tunnel going down, the local BIAS filter might not be updated correctly leading to excess traffic coming to the multihomed device. PR1364410
- While clearing the ARP table or making configuration changes like delete VLAN in a high-scale EVPN VXLAN configuration environment, the routing process on a QFX10000 or QFX5100 might crash causing temporary impact on traffic around the affected node. PR1365257

General Routing

- L3 multicast traffic does not converge 100 percent and a few continuous drops are observed after bringing an interface down and back up again or while an FPC comes online after FPC restart. This behavior is seen when scaling beyond 2000 VLANs or 2000 IRBs with VLAN replication configured. PR1161485
- When per-packet load balancing is removed or deleted, the next-hop index might change. PR1198092
- Because the wrong type was defined from the value drawn from the Packet Forwarding Engine, output for the show interfaces command might show an extremely large number instead of the actual value. Example: **QFX> show interfaces extensive et-0/1/0 Physical interface: et-0/1/0, Enabled, Physical link is Up . Input errors: Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Bucket drops: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 429496729600 <<<<<<<<<<<<<<< Output errors: Carrier transitions: 3, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0, Bucket drops: 0 Where 429496729600 is 6400000000 in hexadecimal**. However, the actual value is 0x64 or 100 in decimal. PR1245748

- Single-bit and multiple-bit ECC errors are not logged on QFX5110 switches. PR1251917
- On QFX10000 line switches, initially the port group module comes up after some time and negative ACKs are seen until the port group module is up. Once the port group module is up, negative ACKs are no longer observed. This is an expected behavior due to an aggressive link scan feature introduced in Junos OS Release 17.2.PR1271579
- On QFX10000 line platforms, with a high scale of 4000 VNIs or 200,000 MACs, or both, if a large configuration change occurs with traffic flowing, then forwarding descriptor memory corruption might occur, leading to complete traffic loss on certain ports. The qualification shows that a system with 400 VNIs has been stable. However, other configurations like global MAC count and underlying MPLS LSPs can increase system load. PR1296089
- In a L2/L3 collapsed EVPN-VXLAN scenario, even though all the remote MACs are learned, more than 60 percent of the traffic is flooded for L2 VNI stretched between PODs with the same subnet but different VLAN-to-VNI mapping even though all the remote MACs are learned. PR1303598
- Traffic drop occurs on sending traffic over "et" interfaces because of the CRC errors. PR1313977
- Port LEDs on QFX5100 do not work. If a device connects to a port on QFX5100, the port LED stays unlit. PR1317750
- There might be traffic loss on the ingress PE device after a new EVPN neighbor is added or an existing EVPN neighbor is deleted. PR1319770
- On a QFX10016, permanent traffic loss is seen for some hosts after the initial ARP timer expires by an ARP entry is not synchronized between the two PE devices. PR1322288
- On the QFX10016 EVPN-VXLAN scaled testbed, it takes up to 3 minutes for traffic to converge when a configuration related to a tenant (5 IRBs/VLAN) is added. PR1323042
- QFX10002-60C filter operation with log action is not supported for protocols other than Layer 2 IPv4 or IPv6 and the message **Protocol 0 not recognized** is seen in firewall logs. PR1325437
- The management process (mgd) might panic after modifying AE interface members under the **ethernet-switching vlan** stanza. As a result, the remote session is terminated. PR1325736
- On the QFX10000, if memory use exceeds the limit, the dcpfe process crashes. PR1329243
- After an IP move, ARP table information is not in sync between two spine devices. PR1330663
- Ingress ACL scale limit need to be increased from 256 to 512 terms. PR1331730
- On the QFX5210, for some UFT profiles, the entries cannot be scaled to 95 percent of the supported scale. PR1332170
- BFD session over AE flaps when a member link carrying the BFD Tx flaps. PR1333307
- On QFX10002-60C, changing MTU for GRE and underlying interfaces in single commit causes the FPC to crash. Refrain from committing MTU changes for GRE and underlying interfaces in single commit. For any GRE interface MTU update follow the mentioned workaround. PR1335739
- VIP address cannot be pinged from back-up when VRRP is configured on subinterfaces qfx10k PR1338256

- On the QFX10002-60C, changing MTU for GRE and underlying interfaces in a single commit might result in an FPC crash. As a workaround to avoid this issue, avoid committing MTU changes for GRE and underlying interfaces together in a single commit. Instead, perform these actions in two separate commits, with some time allowed between the two commits. PR1339601
- When hot swapping a 100G and 40G BiDi optics it is recommended to give a gap of 4 to 5 seconds, for removal and re-insertion event. If the recommended time delay is not provided then the results might be undesirable. PR1356502
- On QFX5110, the FEC for 100G optics is not being displayed when expected behavior is for FEC to be shown as NONE. On QFX10002, the FEC for 40G optics is being displayed as NONE when expected behavior is for FEC not to be displayed. On QFX10008, the FEC for 40G optics is being displayed as NONE when expected behavior is for FEC not to be displayed. PR1360948
- The **clear** command implemented supports QFX10000 platforms. The **clear** command should be used in the following order:
  - **run clear services accounting flow inline-jflow fpc-slot <no>** followed by
  - **run clear services accounting statistics inline-jflow fpc-slot <no>**.PR1362396
- Immediately after AIS script package installation, if any CLI command is executed then no output is generated. PR1368039
- During link configuration at the time of device initialization/bootup, if the MDIO register is corrupted then, the links might not come up. During ZTP, ZTP image upgrade might go through but if you have 40G configurations and are performing a personality switch from PTX --> QFX, post ZTP image upgrade and configuration apply, 40G interfaces might remain down. PR1368203

Interfaces and Chassis

- Configuring the session establishment hold time helps to establish a faster ICCP connection. The recommended value is 50 seconds. PR1328572
- If customers VLAN range is 16 (for example, **vlan-id-list 30-45**) is configured in a Q-in-Q (for example, 802.1ad) scenario, all the 16 VLANs might not pass traffic. PR1345994

Layer 2 Features

- When an FPC encounters a memory exhaustion condition, the FPC restarts unexpectedly with **PPMAN: failed decoding IDL msg - retval -2 type 5 encode_len 208 length 208 data 0x344ff1b0** message. PR1321117

MPLS

- There could be some lingering RSVP state which would keep some labeled-routes programmed in the PFE longer than they should be. This RSVP state will eventually expire and then delete the RSVP MPLS routes from FIB. However, traffic losses is not anticipated due to this lingering state or the corresponding label routes in the FIB. In the worst case, in a network, where there is persistent link flapping going on, this lingering state could interfere with the LSP scale being achieved. PR1331976

Platform and Infrastructure

- Status LED on the chassis does not show up on QFX10002-60C with Junos OS 18.2R1.9 image. Juniper recommends customers to upgrade to Junos OS 18.2R1.10 image and follow up with a jfrmware upgrade with the following command:

  request vmhost system software add /volume/build/junos/18.2/release/18.2R1.10/ship/jfirmware-vmhost-x86-64-18.2R1.10.tgz

  After the jfirmware upgrade, a power cycle is mandatory for the device to be operational in normal state. PR1332991
- Execution of Python scripts through enhanced automation is only supported on non-veriexec images. PR1334425
- On all platforms that support EVPN-VXLAN, if RVTEP is resolved over IRB IP then Routing Engine (RE) does not flood packets, the ARP might not go out and packets might get dropped at Routing Engine. It might cause service impact. PR1348029

Routing Protocols

- For the QFX10002 and QFX10008 switches, you might observe an increase in the convergence time of OSPF routes when compared to Junos OS Release 17.3. An average increase of 1.5 seconds is seen for 100,000 OSPFv3 routes. PR1297541
- Performing GRES on the EVPN-VXLAN topology with uRPF results in total packet loss. PR1322217
- In the PVLAN configuration, the isolated VLAN and community VLAN should not use same VLAN ID. PR1323520

- BGP protocol strongly recommends configuration of local-address for each multihop iBGP or eBGP peer configuration. As a recommendation local-address should be route-able lo0 address. Using loopback address reduces dependency with interfaces. Note: Multihop is by default enabled for iBGP peers. PR1323557
- VLAN range shown in community VLAN is 1..4094. Hence, VLAN 0 should not be configured as community VLAN in PVLAN. PR1323719
- On QFX5200 Virtual Chassis, traffic loss of 0.04 percent is seen with Routing Engine switchover for the GRE tunnel scale test. PR1323884
- QFX10002-60C is not supported as FHR in multicast PIM SM based network. PR1324116
- When MoFRR is enabled, traffic statistics on multicast route shows double the outgoing traffic. Accounting is done for both primary and backup route. When one of the upstream interfaces goes down, this issue is not seen. There is no workaround for this issue. PR1326338
- When cleaning up routes as the peer goes down, we observe a 30% degradation in time taken in Junos OS Release 17.2X75D91 as compared to Junos OS Release 17.2. PR1329921
- Higher convergence time for LFA with BFD in Junos OS Release 18.1. PR1337412

SEE ALSO

New and Changed Features | **196**

Changes in Behavior and Syntax | **204**

Known Behavior | **208**

Resolved Issues | **216**

Documentation Updates | **223**

Migration, Upgrade, and Downgrade Instructions | **223**

Product Compatibility | **237**

Resolved Issues

IN THIS SECTION

This section lists the issues fixed in the Junos OS Release 18.2R1 for the QFX Series.

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

EVPN

- Error message **JPRDS_DLT_ALPHA KHT** shows as failed, but the entries in hardware are programmed correctly. PR1258933
- In an EVPN-VXLAN setup, IPv6 packet loss is observed after normal traffic run rate. PR1267830
- The sub interface from same physical port do not work if configured under same VXLAN VLAN. PR1278761
- When a VLAN uses an IRB interface as the routing interface, the vlan-id parameter must be set to "none" to ensure proper traffic routing. PR1287557
- VXLAN traffic loss is observed after deleting and adding VLANs. PR1318045
- Core link flap might result in an inconsistent global MAC count. PR1328956
- On QFX5100, with EVPN-VXLAN, the leaf device is forwarding traffic to the incorrect VTEP after MAC move/vmotion. PR1335431
- Traffic might be lost on Layer2 and Layer3 spine node in multihome EVPN scenario. PR1355165
- In an EVPN-VXLAN environment, BFD flap causes VTEP to flap and the Packet Forwarding Engine crashes. PR1339084
- The routing protocol process (rpd) crashes and generates a core file on QFX Series switches with multiple VLANs with vlan-id zero, unique VNID. PR1342351
- The traffic might get dropped because the core is down. PR1343515

General Routing

- C0 fiber link does not come up. PR1298876
- Traffic loss might be seen while sending traffic through the 40G interface. PR1309613
- Traffic loss is observed while performing NSSU. PR1311977
- Certain IGMP join packets cannot be processed correctly at a high rate. PR1314382
- Transit traffic over GRE tunnel might hit the CPU and trigger a DDoS violation on the L3 next hop. PR1315773
- Packets such as TDLS without IP header are looped between virtual gateways. PR1318382
- Chassis MIB SNMP OIDs for VC-B member chassis are not available after MX Series Virtual Chassis unified ISSU. PR1320370
- The MAC address get stuck with "DR" flag on the spine node even though packets are received on the interface from source MAC. PR1320724
- The OpenFlow session cannot be established correctly with controller and interfaces options configured on QFX5100 switches. PR1323273
- On a QFX10000 platform deployed in a spine layer without any CE interfaces attached, the ARPs will not get resolved on the spine, and traffic drop might be observed. PR1324739
- The GRE traffic is not decapsulated by the firewall filter. PR1325104
- VLAN or VLAN bridge might not be added or deleted if there is an IFBD HW token limit exhaustion. PR1325217
- Unable to configure persistent learning using CLI **set switch-options interface <interface-name>** because no option is found PR1325313
- MAC move is not expected when disabled globally with CLI **set protocols l2-learning global-mac-move disable-action**. PR1325524
- MAC aging is not happening on lag interface. PR1325555
- ARP request packets might not be flooded on QFX5110. PR1326022
- On QFX5210, when the physical interface is down, the CLI **show chassis LED** still shows "Green". PR1326078
- The major alarm about **Fan and PSU Airflow direction mismatch** might be seen by removing the management cable. PR1327561
- Deleting one VXLAN might cause traffic loop on another VXLAN in a multihoming EVPN and VXLAN scenario with the service provider style interface. PR1327978
- On QFX10002, a major alarm should be cleared once the chassis has more PEM units installed than the "minimum PEM" configuration. PR1327999
- A FAN tray removal or insertion trap is not generated for the backup FPC. PR1329031

- IRB physical interface static MAC address is not taking effect. PR1329032
- The CLI command **set chassis fpc 0 pic** has an option of PIC numbers 0 to 2, but the hardware only has one PIC. PR1329105
- The etherStatsCRCAlignErrors port counters might disappear in the SNMP tree. PR1329713
- After commit, members of Virtual Chassis or VCF are split and some members might get disconnected. PR1330132
- The rpd generates a core file on new backup Routing-Engine at **task_quit,task_terminate_timer_callback,task_timer_dispatch,task_scheduler after disabling NSR+GRES**. PR1330750
- On QFX10002-36Q, DHCP relay or server not working on GRE interface. PR1331158
- PTP BC with its PTP slave interface configured on a 100-Gigabit Ethernet interface might get stuck in FREERUN state. PR1331752
- Adding or deleting a tunnel configuration might result in FPC crash in a scaled GRE tunnels scenario. PR1331983
- On QFX5210, for some of the UFT profiles, the UFT is not able to scale the s,g entries to around 95 percent of the supported scale. PR1332170
- The error messages **out of HMC range** and **HMC READ faild** are seen. PR1332251
- Traffic does not flow through VCP ports after rebooting the Virtual Chassis members. PR1332515
- In an EVPN-VXLAN environment, DF drops multicast traffic. PR1333069
- The SDHCPv6 SOLICIT message is dropped. PR1334680
- Ethernet frame with Ethernet type of 0x8922 might be modified at egress by QFX10000. PR1334711
- The chassis reboots continuously when USB drive is connected after image recovery through USB and after CLI image install. PR1335269
- The supported scale for logical interface-based GRE tunnel on QFX10002-60C is 512. PR1335681
- The CLI command for beacon port state is not supported on QFX10002-60C. PR1337125
- SNMP jnxBoxDescr oid returns different value when upgrading to Junos OS Release 17.2. PR1337798
- The traffic coming from the remote VTEP PE device might get dropped. PR1338532
- The analyzer status might show as down when port mirroring is configured to mirror packets from an aggregated Ethernet member. PR1338564
- The VXLAN traffic might not be transmitted correctly with IRB interface as underlay interface of VTEP tunnel. PR1338586
- Reduced multicast scale with downstream IRB interfaces with snooping enabled. PR1340003
- Inconsistent result is seen in QFX5200 after using **deactivate xxx** command in pfc-priority and no-loss context. PR1340012

- IPv4 traffic routed out through incorrect interface after rpd restarts in leaf of IPCLOS profile. PR1341381
- In an EVPN-VXLAN, L3 traffic is not getting converged properly upon disabling the ECMP link between the spine and the leaf with EVPN-VXLAN configurations. PR1343172
- BPDU packets might get dropped and **bpdu-block-on-edge** might not work. PR1343330
- Broadcast frames might be modified with the ethertype 0x8850. PR1343575
- In an EVPN/VXLAN, VLAN with flexible-tag mode, the xe statistics is not updated for ingress. PR1343746
- Implement **[edit interfaces interface-name ether-options] configured-flow-control** option for QFX Series switches. PR1343917
- EVPN-VXLAN: ARP packet uses VRRP/virtual-gateway MAC in Ethernet header instead of IRB MAC address. PR1344990
- QFX5100 - Fan RPM fluctuates when temperature sensor reaches its threshold. PR1345181
- FXPC process might generate a core file while removing a VXLAN configuration. PR1345231
- Incorrect inner VLAN tag is sent from QFX10000 platform with Q-in-Q configured on the Layer3 sub-interface. PR1346371
- In QFX10000 SFlow scaling scenario, error messages are seen in syslog messages with respect to SFlow after configuring multiple LAG interfaces under SFlow protocol. PR1346493
- On QFX5100, in an EVPN a DCPFE core file is generated at **src/pfe/common/pfe-arch/brcm/applications/virtual/brcm_vxlan.c:2185**. PR1346980
- QFX5100-48T 10G interface might be auto-negotiated at 100M speed instead of 10G. PR1347144
- The IPFIX flow statistics are incorrect in the exported record. PR1347229
- Part numbers and serial numbers are not displayed for any of the 10G optics or DAC connected. PR1347634
- QFX10000 systems might encounter a chassis alarm indicating **FPC 0 Major Errors - PE Error code: 0x2100ba**. PR1347805
- Once in QFX10002-60C VMHOST crash is observed at prds_if_ifl_get_gre_stats (ifl=0x9288a608, expr_ifl_l2d_stats=0x2cd3790c), just after configuring GR interface on it. PR1348932
- The pfed process consumes 80 to 90 percent CPU running subscriber management on PPC-based routers. PR1351203
- DCPFE process might crash on QFX10000 switches. PR1351503
- The GTP traffic might not be hashed correctly for AE interface. PR1351518
- RPC output not showing failure when running **request system software add** with software already staged. PR1353466
- SFP-LX10 stay in up or down when connected. PR1353677
- The alarm errors might be seen during the bootup on QFX10000. PR1354582

- Untagged packets might not be forwarded through the trunk port. PR1355338
- On QFX5110 platforms, LX10 SFP needs to be reinserted after autonegotiation is enabled or disabled. PR1355746

Interfaces and Chassis

- If customer virtual local area network (CVLAN) range-16 (for example, vlan-id-list 30-45) is configured in a Q-in-Q (802.1ad) scenario, all the 16 VLANs might not pass traffic. PR1345994

Junos Fusion Satellite Software

- AD failure (power off) in a DC fusion is causing complete or partial traffic loss for extended period. PR1352167

Layer 2 Features

- MAC learning might fail for device on extended port of satellite device after MAC moving in a Junos Fusion scenario. PR1324579
- The DHCP discover packets might be looped in an MC-LAG and DHCP-Relay scenario. PR1325425
- In QFX5100, with multiple logical units configured on an interface, **input-vlan-map POP** does not remove outer vlan-tag when Q-in-Q and VXLAN are involved. PR1331722
- Push is not working for VXLAN local switching with the Q-in-Q. PR1332346
- Interface with **flexible-vlan-tagging** and **family ethernet-switching** does not work on QFX10000. PR1337311
- The DCPFE/FXPC process might crash and generate a core file. PR1362332

MPLS

- In a QFX5100, a unified ISSU is not supported with MPLS configuration. PR1264786
- A traffic drop is seen during NSR switchover for RSVP P2MP provider tunnels used by MVPN. PR1293014
- MPLS forwarding might not happen properly for some LSPs. PR1319379
- The rpd might crash on the backup Routing Engine because of memory exhaustion. PR1328974
- The hot standby for l2 circuit does not work on QFX5000. PR1329720

Multicast

- An aggregated Ethernet or IRB configuration causes kernel crash vmcore , and causes chassis or FPC reboot. PR1335904

Platform and Infrastructure

- The ARP might not update, and packets might get dropped at the Routing Engine. PR1348029
- When a Junos OS image is shipped with translation scripts downgrading to another image, stale symlinks of translation scripts at the time of mgd initialization leads box going into amnesiac state. PR1341650

Routing Protocols

- The **copy-tos-to-outer-ip-header** command is not supported, because of the hardware limitation. PR1313311
- Some of the IPv4 multicast routes in the Packet Forwarding Engine might fail to install and update. PR1320723
- In QFX5100, consistent hashing is not getting programmed. PR1322299
- QFX10002-60C is not supported as FHR in multicast PIM SM based network. PR1324116
- IS-IS L2 Hello packets are dropped when they come from a Brocade device. PR1325436
- Degradation is seen in some OSPF parameters and some of the RIB parameters are improved. PR1329921
- The loopbacked IRB interface is not accessible to the remote network. PR1333019
- The dcpfe crashes in a route leak scenario on QFX10000. PR1334714
- The rpf-check-policy does not work as expected. PR1336909
- On QFX5000 Series switches, BGP might be down due to the congestion state of CPU on receiving Ethernet pause frames. PR1343597
- DF is not working; ping fails if MTU is different on the interfaces. PR1345495
- The vrf-fallback on QFX5000 is not supported in ALPM mode. PR1345501
- IPv6 packets with hop-by-hop header cannot be matched using filters. PR1346052

SEE ALSO

New and Changed Features | **196**

Changes in Behavior and Syntax | **204**

Documentation Updates

There are no errata or changes in Junos OS Release 18.2R1 documentation for the QFX Series.

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 **18.2** in the Release pull-down list to the right of the Software tab on the Download Software page.

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 18.2 release.

   An Alert box appears.

5. In the Alert box, click the link to the PSN document for details about the software, and click the link to download it.

   A login screen appears.

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

7. Download the software to a local host.

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

9. Install the new jinstall package on the device.

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

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

```
user@host> request system software add
source/jinstall-host-qfx-5-x86-64-18.2-R1.n-secure-signed.tgz reboot
```

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

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

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

Rebooting occurs only if the upgrade is successful.

> **NOTE:** After you install a Junos OS Release 18.2 **jinstall** package, you can issue the **request system software rollback** command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

This section explains how to upgrade the software, which includes both the host OS and the Junos OS. This upgrade requires that you use a VM host package—for example, a **junos-vmhost-install-x.tgz** .

During a software upgrade, the alternate partition of the SSD is upgraded, which will become primary partition after a reboot .If there is a boot failure on the primary SSD, the switch can boot using the snapshot available on the alternate SSD.

> **NOTE:** The QFX10002-60C switch supports only the 64-bit version of Junos OS.

> **NOTE:** If you have important files in directories other than /config and /var, copy the files to a secure location before upgrading. The files under /config and /var (except /var/etc) are preserved after the upgrade.

To upgrade the software, you can use the following methods:

If the installation package resides locally on the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-18.2R1.9.tgz
```

If the Install Package resides remotely from the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add
ftp://ftpserver/directory/junos-vmhost-install-qfx-x86-64-18.2R1.9.tgz
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Installing the Software on QFX10002 Switches

NOTE: If you are upgrading from a version of software that does not have the FreeBSD 10 kernel (15.1X53-D30, for example), you will need to upgrade from Junos OS Release 15.1X53-D30 to Junos OS Release 15.1X53-D32. After you have installed Junos OS Release 15.1X53-D32, you can upgrade to Junos OS Release 15.1X53-D60 or Junos OS Release 18.2R1.

NOTE: On the switch, use the **force-host** option to force-install the latest version of the Host OS. However, by default, if the Host OS version is different from the one that is already installed on the switch, the latest version is installed without using the **force-host** option.

If the installation package resides locally on the switch, execute the **request system software add *<pathname><source>* reboot** command.

For example:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-f-x86-64-18.2R1.n-secure-signed.tgz reboot
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* reboot** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-f-x86-64-18.2R1.n-secure-signed.tgz reboot
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches

> **NOTE:** Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

The switch contains two Routing Engines, so you will need to install the software on each Routing Engine (re0 and re1).

If the installation package resides locally on the switch, execute the **request system software add *<pathname><source>*** command.

To install the software on re0:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* re0** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

To install the software on re1:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* re1** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

Reboot both Routing Engines.

For example:

```
user@switch> request system reboot both-routing-engines
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Installing the Software on QFX10008 and QFX10016 Switches

Because the switch has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

WARNING: If graceful Routing Engine switchover (GRES), nonstop bridging (NSB), or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you issue the CLI **delete chassis redundancy** command when prompted. If GRES is enabled, it will be removed with the **redundancy** command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the **[edit routing-options]** hierarchy level to disable it.

1. Log in to the master Routing Engine's console.

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

2. From the command line, enter configuration mode:

   ```
   user@switch> configure
   ```

3. Disable Routing Engine redundancy:

   ```
   user@switch# delete chassis redundancy
   ```

4. Disable nonstop-bridging:

   ```
   user@switch# delete protocols layer2-control nonstop-bridging
   ```

5. Save the configuration change on both Routing Engines:

   ```
   user@switch# commit synchronize
   ```

6. Exit the CLI configuration mode:

   ```
   user@switch# exit
   ```

After the switch has been prepared, you first install the new Junos OS release on the backup Routing Engine, while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the software version on the other Routing Engine.

7. Log in to the console port on the other Routing Engine (currently the backup).

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

8. Install the new software package using the **request system software add** command:

   ```
   user@switch> request system software add validate
   /var/tmp/jinstall-host-qfx-10-f-x86-64-18.2R1.n-secure-signed.tgz
   ```

   For more information about the **request system software add** command, see the CLI Explorer.

9. Reboot the switch to start the new software using the **request system reboot** command:

   ```
   user@switch> request system reboot
   ```

   > **NOTE:** You must reboot the switch to load the new installation of Junos OS on the switch.
   >
   > To abort the installation, do not reboot your switch. Instead, finish the installation and then issue the **request system software delete *<package-name>*** command. This is your last chance to stop the installation.

   All the software is loaded when you reboot the switch. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

   While the software is being upgraded, the Routing Engine on which you are performing the installation is not sending traffic.

10. Log in and issue the **show version** command to verify the version of the software installed.

    ```
    user@switch> show version
    ```

    Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the master Routing Engine software.

11. Log in to the master Routing Engine console port.

    For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

12. Transfer routing control to the backup Routing Engine:

    ```
    user@switch> request chassis routing-engine master switch
    ```

    For more information about the **request chassis routing-engine master** command, see the CLI Explorer.

13. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

    ```
    user@switch> show chassis routing-engine
    Routing Engine status:
      Slot 0:
        Current state                  Backup
        Election priority              Master (default)
    Routing Engine status:
      Slot 1:
        Current state                  Master
        Election priority              Backup (default)
    ```

14. Install the new software package using the **request system software add** command:

    ```
    user@switch> request system software add validate
    /var/tmp/jinstall-host-qfx-10-f-x86-64-18.2R1.n-secure-signed.tgz
    ```

    For more information about the **request system software add** command, see the CLI Explorer.

15. Reboot the Routing Engine using the **request system reboot** command:

```
user@switch> request system reboot
```

> **NOTE:** You must reboot to load the new installation of Junos OS on the switch.
>
> To abort the installation, do not reboot your system. Instead, finish the installation and then issue the **request system software delete jinstall *<package-name>*** command. This is your last chance to stop the installation.

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation does not send traffic.

16. Log in and issue the **show version** command to verify the version of the software installed.

17. Transfer routing control back to the master Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the **request chassis routing-engine master** command, see the CLI Explorer.

18. Verify that the master Routing Engine (slot 0) is indeed the master Routing Engine:

```
user@switch> show chassis routing-engine
```

```
Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)
outing Engine status:
  Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
```

Performing a Unified ISSU

You can use unified ISSU to upgrade the software running on the switch with minimal traffic disruption during the upgrade.

NOTE: Unified ISSU is supported in Junos OS Release 13.2X51-D15 and later.

Perform the following tasks:

- Preparing the Switch for Software Installation on page 234
- Upgrading the Software Using Unified ISSU on page 234

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

- Ensure that nonstop active routing (NSR), nonstop bridging (NSB), and graceful Routing Engine switchover (GRES) are enabled. NSB and GRES enable NSB-supported Layer 2 protocols to synchronize protocol information between the master and backup Routing Engines.

  To verify that nonstop active routing is enabled:

  NOTE: If nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

  ```
  user@switch> show task replication
          Stateful Replication: Enabled
          RE mode: Master
  ```

  If nonstop active routing is not enabled (**Stateful Replication** is **Disabled**), see *Configuring Nonstop Active Routing on Switches* for information about how to enable it.

- Enable nonstop bridging (NSB). See *Configuring Nonstop Bridging on Switches (CLI Procedure)* for information on how to enable it.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the **request system snapshot** command.

Upgrading the Software Using Unified ISSU

This procedure describes how to upgrade the software running on a standalone switch.

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in *Installing Software Packages on QFX Series Devices*.
2. Copy the software package or packages to the switch. We recommend that you copy the file to the **/var/tmp** directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:
   - On the switch, enter:

     ```
     user@switch> request system software in-service-upgrade /var/tmp/package-name.tgz
     ```

     where ***package-name*.tgz** is, for example, **jinstall-host-qfx-10-f-x86-64-18.2R1.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-x86-64-18.2R1.n-secure-signed.tgz ...
     Install jinstall-host-qfx-5-f-x86-64-18.2R1.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

- New and Changed Features | **196**
- Changes in Behavior and Syntax | **204**
- Known Behavior | **208**
- Known Issues | **211**
- Resolved Issues | **216**
- Documentation Updates | **223**
- Product Compatibility | **237**

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | **237**

Hardware Compatibility

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

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

Hardware Compatibility Tool

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

SEE ALSO

Junos OS Release Notes for SRX Series

IN THIS SECTION

These release notes accompany Junos OS Release 18.2R1 for the SRX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

New and Changed Features

IN THIS SECTION

This section describes the new features and enhancements to existing features in Junos OS Release 18.2R1, Junos OS Release 18.2R1-S1 and Junos OS Release 18.2R1-S3 for the SRX Series devices.

Junos OS Release 18.2R1 supports the following Juniper Networks security platforms: vSRX, SRX300/320, SRX340/345, SRX550HM, SRX1500, SRX4100/4200, SRX4600, SRX5400, SRX5600, and SRX5800. Most security features in this release were previously delivered in Junos OS for SRX Series “X” releases from 12.1X44 through 15.1X49-D130. Security features delivered in Junos OS for SRX Series “X” releases after 15.1X49-D130 are not available in 18.2 releases.

Junos OS Release 18.2R1-S1 and Junos OS Release 18.2R1-S3 supports SRX5K-SPC3. Junos OS for SRX Series documentation includes information about SRX5K-SPC3.

New features for security platforms in Junos OS Release 18.2R1, Junos OS Release 18.2R1-S1 and Junos OS Release 18.2R1-S3 include:

Release 18.2R1-S3 New and Changed Features

VPN

- **IPsec VPN support on SRX5K-SPC3 card (SRX5400, SRX5600, SRX5800)**—Starting in Junos OS Release 18.2R1-S3, SPC3 card supports IPsec VPN with AutoVPN networks in point-to-point secure tunnel mode with multiple traffic selectors, Dead peer detection (DPD), IKE fragmentation, and Site-to-site VPN (responder only).

  For SPC3 cards, you can only verify the tunnel mapping on different SPUs using the **show security ipsec tunnel-distribution** command. You can continue to use **show security ike tunnel-map** command to view the tunnel mapping on different SPUs with SPC2.

  The **show security ipsec tunnel-events-statistics** command is not supported on SPC3 card.

  [See show security ipsec security-associations.]

Release 18.2R1-S1 New and Changed Features

Hardware

- **SRX5K-SPC3 Card support (SRX5400, SRX5600, SRX5800)**—Starting with Junos OS Release 18.2R1-S1, SRX5K-SPC3 Services Processing Cards (SPCs) are available on SRX5400, SRX5600, and SRX5800 Services Gateways. SRX5K-SPC3 card provides additional processing power to run integrated services such as firewall, IPSec, and IDP. The SRX5K-SPC3 contains two Services Processing Units (SPUs) with 128GB of memory per SPU. All traffic traversing the services gateway is intelligently distributed by I/O cards (IOCs) to the SPUs to have services processing applied to it.

  [See SRX5400 Services Gateway Hardware Guide, SRX5600 Services Gateway Hardware Guide, SRX5800 Services Gateway Hardware Guide, and SRX5400, SRX5600, and SRX5800 Services Gateway Card Reference.]

Interfaces and Chassis

- **User visibility improvements for chassis environment CLI (SRX5400, SRX5600, SRX5800)**—Starting in Junos OS Release 18.2R1-S1, the **show chassis environment fpc** CLI command displays current and power for SPC3 board along with the FPC voltage. In the earlier releases, only FPC voltage was displayed.

  [See show chassis environment.]

J-Web

- **J-Web supports SRX5K-SPC3 Card**—Starting Junos OS Release 18.2R1-S1, J-Web is enhanced to show SRX5K-SPC3 card support for SRX5400, SRX5600, and SRX5800 devices.

Platform and Infrastructure

- **SRX5K-SPC3 card (SRX5400, SRX5600, SRX5800)**—Starting in Junos OS Release 18.2R1-S1, a new service processing card (SRX5K-SPC3) is introduced for the SRX5000 line of devices. The introduction of the new card improves the scalability and performance of the device and maintains its reliability as it

preserves the chassis cluster functionality. The SRX5K-SPC3 card supports higher bandwidth for service processing. It provides support for the following software features:

- Application layer gateway (ALG)
- Advanced anti-malware (Juniper Sky ATP)
- Application security suite
- Flow-based packet processing implementation
- GPRS tunneling protocol (GTP) and stream control transmission protocol (SCTP)
- High availability (chassis cluster)
- Intrusion detection and prevention (IDP)
- J-Web
- Network address translation (NAT)
- Stateful firewall
- SSL proxy
- Firewall user authentication
- UTM (antivirus, web filtering, content filtering, and antispam)

NOTE:

The following limitations apply for the SPC3 card in Junos OS Release 18.2R1-S1:

- Interoperability of SPC2 card and SPC3 card is not supported.
- IPsec VPN functionality is not supported with SPC3 card.

[See Understanding Flow support on SRX5K-SPC3 Platforms,Monitoring of Global-Level Objects in a Chassis Cluster, and Persistent NAT and NAT64.]

Release 18.2R1 New and Changed Features

ALG

- **TWAMP supports for ALG traffic (SRX Series)**—Starting in Junos OS Release 18.2R1, the Two-Way Active Measurement Protocol (TWAMP) Application Layer Gateway (ALG) is supported to enable the TWAMP data traffic to pass through the SRX Series device without needing a predefined policy permission.

  [See Understanding the Two-Way Active Measurement Protocol (TWAMP) Application Layer Gateway (ALG).]

Application Security

- **Application Quality of Experience (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100 and SRX4200, vSRX)**—Starting in Junos OS Release 18.2R1, AppQoE enables you to effectively prioritize, segregate, and route business-critical applications traffic without compromising performance or availability.

  AppQoE utilizes the capability of application identification and advanced policy-based routing to identify specific applications in the network and to specify a path for the application traffic according (service-level agreement) SLA rules.

  AppQoE monitors RTT, jitter, and packet loss on each link, and based on the score, seamlessly diverts applications to an alternate path if the performance of the primary link is below acceptable levels as specified by the SLA. Measurement and monitoring of application performance is done using active and passive probes, which detect SLA violations and help select an alternate path for that particular application.

  [SeeApplication Quality of Experience.]

- **Support for advanced policy-based routing (APBR) policy (SRX Series, vSRX)**—Starting in Junos OS Release 18.2R1, you can configure advanced policy-based routing (APBR) policies by defining source addresses, destination addresses, and applications as match conditions; and after a successful match, the configured APBR profile is applied as an application service for the session.

  In previous releases of Junos OS, an APBR profile could be attached to an incoming security zone of the ingress traffic, and the APBR was applied only on the basis of the security zone.

  This enhancement provides more flexible traffic-handling capabilities that offer granular control for forwarding packets.

  [See Advanced Policy-Based Routing.]

Authentication and Access Control

- **Support for user firewall to configure ClearPass and JIMS at the same time (SRX Series, vSRX)**—Starting in Junos OS Release 18.2R1, you can configure ClearPass and Juniper Identity Management Service (JIMS) at the same time. By configuring ClearPass and JIMS at the same time, SRX Series devices can

query JIMS for user identification entries, and ClearPass can push device entries to the SRX Series device through the Web API. In releases before Junos OS Release 18.2R1, you are restricted to configure either ClearPass or JIMS.

[See Understanding How ClearPass and JIMS Works at the Same Time.]

- **Enhancement to NTP authentication method (SRX300, SRX320, SRX340, SRX345, and SRX550M)**—Starting in Junos OS Release 18.2R1, Junos OS supports NTP authentication for both SHA-1 and SHA2-256, in addition to the existing NTP authentication method, MD5. You can now choose from among MD5, SHA-1, and SHA2-256 for synchronizing the clocks of Juniper Network routers, switches, and other security devices on the Internet. Using SHA-1 instead of MD5 improves the security of devices with very little impact to timing, while using SHA2-256 provides an increase in security over SHA-1.

  NOTE: By default, network time synchronization is unauthenticated.

  To implement authentication, use **set authentication-key *<key_number>* type** at the **[edit system ntp]** hierarchy level.

  - To enable SHA-1 authentication, use **set authentication key *<key_number>* type sha1 value *<password>*** at the **[edit system ntp]** hierarchy level.
  - To enable SHA2-256 authentication, use **set authentication key *<key_number>* type sha256 value *<password>*** at the **[edit system ntp]** hierarchy level.

  [See authentication-key and Configuring NTP Authentication Keys.]

Flow and Processing

- **Reverse Route with Packet Mode (SRX Series)**—Starting from Junos OS Release 18.2R1, the reverse route using virtual router is supported with the new CLI command **set security flow advanced-options reverse-route-packet-mode-vr**. While processing the traffic from the server to the client, if the route of the traffic is changed, the traffic is rerouted using the virtual router from the packet incoming interface or filter-based forwarding.

  [See Understanding Reverse Route Packet Mode Virtual Router.]

IDP

- **Flexible grouping of IDP signatures for policies and profiles (SRX Series)**—Starting with Junos OS Release 18.2R1, IDP signature updates support four new tags for creating more sophisticated dynamic groups in addition to the existing seven tags. The signature database is one of the major components of intrusion detection and prevention (IDP). It contains definitions of different objects—such as attack objects, application signatures objects, and service objects—that are used in defining IDP policy rules. Attacks can be grouped by set of tags.

The additional tags are:

- CVSS Score (for example, All signatures above 8.0)
- Age (for example, Older than <x> years)
- File Type (for example, MPEG, MP4, PPT, and *.doc)
- Vulnerability Type (for example, buffer overflow, injection, use after free, XSS, and RCE)

The Product and Vendor tags are already supported under existing filter products. The CLI interface for configuring these tags is now been made more user friendly with possible completions being available for configuration.

- Vendor (for example, Microsoft, Apple, Red Hat, Google, Juniper, Cisco, and Oracle)
- Product (for example, Office, Database, Firefox, Chrome, Flash, DirectX, Java, and Kerberos)

[See IDP Policy Rules and IDP Rule Bases.]

Interfaces and Chassis

- **100G Interfaces Support (SRX4600)**–Starting in Junos OS Release 18.2R1, SRX4600 devices support 4x100G Ethernet mode using QSFP28 transceivers. To enable 100-Gigabit Ethernet on the marked ports, use the **set chassis fpc** command.

  [See SRX4600 Gateway Rate-Selectability.]

J-Web

- **J-Web support for Unified L4/L7 Firewall Policy**—Starting Junos OS Release 18.2R1, J-Web supports unified L4/L7 firewall policy, where in you can configure current AppFW by applying its matching criteria of rules to the policy. Also, there are changes to UTM, IPS, AppID, SSL Proxy, Flow and Service redirect.
- **J-Web support for Logical Systems**—Starting Junos OS Release 18.2R1, J-Web supports Logical Systems in SRX5400, SRX5600, and SRX5800 devices, providing multi-tenant firewalls by logically partitioning a single physical firewall into multiple logical systems with separate networking and security services.
- **J-Web support for Configuring ICAP Redirect and SSL Initiation Profiles**—Starting Junos OS Release 18.2R1, using J-Web you can configure ICAP redirect profile and SSL initation profile, which enables you to decrypt HTTPS traffic and redirect HTTP message to 3rd party on-premise DLP server via ICAP/SICAP channel.
- **J-Web Enhanced Look and Feel**—Starting Junos OS Release 18.2R1, J-Web for SRX5400, SRX5600, and SRX5800 devices will have a new and enhanced look and feel.
- **J-Web Configuration Commit Enhancement**—Starting Junos OS Release 18.2R1, after you commit a new J-Web configuration, you can test the configuration for a time period and confirm the commit or roll back to the previous configuration.
- **J-Web support for Logical Domain Interconnect and Routing Instance**—Starting Junos OS Release 18.2R1, using J-Web you can configure the interconnect between logical interfaces and between the

root domain and logical systems. Based on the interconnection, you can configure LT interface unit, peer unit, logical system or VPLS switch, and IP addresses for logical system LT interface.

Logical Systems

- **Enabling or disabling ALGs in logical systems (SRX Series)**—Starting in Junos OS Release 18.2R1, you can enable or disable the configuration of Application Layer Gateways (ALGs) in each logical system individually and view the status of the ALGs for all logical systems or specific logical systems. All 12 data ALGs (DNS, FTP, TFTP, MSRPC, SUNRPC, PPTP, RSH, RTSP, TALK, SQL, IKE, and TWAMP) and four VOIP ALGs (SIP, H.323, MGCP, and SCCP) are supported on logical systems.

  [See Understanding Application Layer Gateway (ALG) in Logical System.]

- **Flow enhancement for interconnect logical system (SRX Series)**—Starting in Junos OS Release 18.2R1, the interconnect logical system routing and scaling are supported. You can interconnect multiple logical systems and multiple VPLS switches to pass the traffic without exiting the device. The logical tunnel interface point-to-point connection **encapsulation frame-relay, encapsulation ethernet** is introduced to optimize the obtainability of logical systems. The frame relay encapsulation adds data-link connection identifier (DLCI) information to the given frame.

  [See SRX Series Logical System Master Administrator Configuration Tasks Overview.]

- **Logical systems support (SRX4100 and SRX4200)**—Starting in Junos OS Release 18.2R1, the logical systems are supported on SRX4100 and SRX4200 devices in addition to the existing support on SRX Series devices such as SRX1500, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800.

  [See Understanding Logical Systems for SRX Series Services Gateways.]

- **Logging support (SRX Series, vSRX)**—Starting in Junos OS Release 18.2R1, the off-box logging (stream mode) service is virtualized. Hence the off-box logging configuration is supported for each logical system and logs are handled based on these configurations. The **[edit logical-system logical-system-name security log]** command is introduced for virtualized logging support. The stream mode is a set of logging services that includes:

  - Off-box logging (SRX Series)
  - On-box logging and reporting (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX)

  [See Understanding Security Logs and Logical Systems.]

- **User firewall enhanced support with logical systems (SRX Series)**—Starting in Junos OS Release 18.2R1, support for user firewall authentication is enhanced using a shared model. In this model, user logical systems share user firewall configuration and authentication entries with the root logical system.

  [See Understanding Integrated User Firewall support in a Logical System.]

- **User logical system support for Layer 2 (SRX Series)**—Starting in Junos OS Release 18.2R1, the user logical system is supported for Layer 2 traffic and firewall session on SRX4100 and SRX4200 devices.

  [See Example: Configuring User Logical Systems Security Profiles.]

NAT

- **Network Address Translation (NAT) support for logical systems (SRX1500, SRX4100, SRX4200)**—Starting in Junos OS Release 18.2R1, the NAT functionality is supported for logical systems on SRX1500, SRX4100, and SRX4200 devices in addition to existing support on SRX5400, SRX5600, and SRX5800. NAT is a method for modifying or translating network address information in packet headers. Either source or destination addresses or both in a packet can be translated. NAT can include the translation of port numbers as well as IP addresses.

  [See Understanding Logical System Network Address Translation.]

Routing and Forwarding Options

- **NDP and DAD Proxy Support (SRX Series)**—Starting in Junos OS Release 18.2R1, SRX Series devices support Neighbor Discovery Protocol (NDP) and Duplicate Address Detection (DAD) proxy features at the interface level. The NDP and DAD proxies are required if hosts in the same subnet are restricted from communicating directly with each other and need to use the proxy node to forward the packets between them. This feature is primarily used in scenarios where the proxying node needs to apply access control and intercept the traffic flowing between the hosts.

  [See Configuring Duplicate Address Detection Proxy and Configuring Neighbor Discovery Protocol Proxy.]

Security Policies

- **Support for unified policies (SRX Series and , vSRX instances)**—Starting in Junos OS Release 18.2R1, unified policies are now supported on SRX Series devices and vSRX instances, allowing granular control and enforcement of dynamic Layer 7 applications within the traditional security policy.

  Unified policies are the security policies, where you can use dynamic applications as match conditions along with existing 5-tuple or 6-tuple matching conditions (with user firewall) to detect application changes over time, and allow you to enforce a set of rules for the transit traffic.

  Unified policies allow you to use dynamic application as one of the policy match criteria rule in each application. Application identification (AppID) is applied on the traffic, and the application is identified after several packets are checked.

  Before identifying the final application, the policy cannot be matched precisely. A potential policy list is made available, and the traffic is permitted using the potential policy from the list.

  After the application is identified, the final policy is applied to the session. Policy actions such as permit, deny, reject, or redirect is applied on the traffic as per the policy rules.

  [See Understanding Unified Policies.]

The following features support unified policies:

- **Application Identification (AppID)**—Unified policy leverages the application identity information from the Application Identification (AppID). AppID provides the information such as dynamic application classification, default protocol and port of an application. For any application included in the dependent list of another application, AppID provides this information.

  [See Application Identification.]

- **Application firewall (AppFW)**—Unified policy configuration handles AppFW functionality and simplifies the task of configuring firewall policy to permit or block application traffic from the network.

  If you configure a unified policy with a dynamic application as one of the matching conditions, then the configuration eliminates the additional steps involved in AppFW configuration—that is, configuring a security policy to invoke the application firewall service.

  Starting in Junos OS Release 18.2R1, the Application Firewall (AppFW) functionality is deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

  The **[edit security application-firewall]** hierarchy level and all configuration options under this hierarchy are deprecated.

  [See Application Firewall.]

- **Application Quality of Service (AppQoS)**—AppQoS functionality is supported when the device is configured with unified policies. You can configure a default AppQoS rule set to manage unified policy conflicts, if multiple security policies match the traffic.

  [See Application Quality of Service.]

- **ICAP service redirect**—Internet Content Adaptation Protocol (ICAP) service redirect functionality is supported when the device is configured with unified policies.

  [See iCAP Service Redirect.]

- **IDP**—Starting with Junos OS Release 18.2R1, with unified policies support, when a security rule has IDP enabled, the name of the actual IDP policy is replaced. This is to simplify IDP policy usage and to provide flexibility to have multiple policies active at the same time.

  All IDP matches will now be handled within the unified policies. As a part of session interest check IDP will enabled if IDP policy is present in any of the matched rules.

  IDP policy is activated in security policies, by permitting the IDP policy within the application services using the **set security policies from-zone zone-name to-zone zone-name policy policy-name then permit application-services idp-policy idp-policy-name** command.

  Since IDP policy name is directly use in the security policy rule, the **[edit security idp active-policy policy-name]** statement is deprecated.

  [See IDP Policies Overview.]

- **SSL proxy**—SSL proxy functionality is supported when the device is configured with unified policies. You can configure a default SSL proxy profile to manage unified policy conflicts, if multiple security policies match the traffic.

  [See SSL Proxy.]

- **UTM**—A new dynamic application policy match condition is added to SRX Series devices, allowing an administrator to more effectively control the behavior of Layer 7 applications. To accommodate Layer 7 application-based policies in UTM, the **[edit security utm default-configuration]** command is introduced. If any parameter in a specific UTM feature profile configuration is not configured, then the corresponding parameter from the UTM default configuration is applied.

  Additionally, during the initial policy lookup phase which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list which contains different UTM profiles, the SRX Series device applies the default UTM profile until a more explicit match has occurred.

  [See Understanding Unified Policies [Unified Threat Management (UTM)].]

- **Juniper Sky ATP support within unified policy (SRX Series)**— Juniper Sky ATP is supported for unified policies. The **set services security-intelligence default-policy** and **set services advanced-anti-malware default-policy** commands are introduced to create default settings for both policy types. During the initial policy lookup phase, which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list, which contain different security intelligence or anti-malware policies, the SRX Series device applies the default policy until a more explicit match has occurred.

  [See the Juniper Sky ATP Administration Guide.]

User Interface and Configuration

- **Support for displaying ephemeral configuration data with filtering (SRX Series)**—Starting in Junos OS Release 18.2R1, the **show ephemeral-configuration** command enables you to specify the scope of the configuration data to display. To filter the displayed configuration data, append the statement path of the requested hierarchy to the command.

  [See Displaying Ephemeral Configuration Data in the Junos OS CLI.]

UTM

- **Antispam supports IPv6 address [SRX Series]** —Starting in Junos OS Release 18.2R1, the antispam feature supports IPv6 traffic.

  [See Antispam Filtering.]

VPN

- **Configuring forwarding class on IPsec VPNs (SRX Series, vSRX)**—Starting with Junos OS Release 18.2R1, forwarding classes configured on an SRX Series device can be mapped to IPsec security associations

(SAs). Multiple IPsec SAs are negotiated on the same IKE SA with a peer device, one SA per forwarding class configured in IPsec.

A unique IPsec SA is negotiated with the VPN peer for each forwarding class. By mapping the forwarding class to the IPsec SA, all the packets with a certain class-of-service (CoS) value will get quality-of-service (QoS) treatment between the peer devices thus avoiding packet drop due to the anti-replay window. This feature provides QoS for IPsec when peer devices allow for multiple SA negotiation.

[See Understanding CoS-Based IPsec VPNs with Multiple IPsec SAs.]

- **Public key infrastructure (PKI) proxy support (SRX Series)**—Starting in Junos OS Release 18.2R1, PKI supports Hypertext Transfer Protocol (HTTP) Web proxy. HTTP Web proxy acts as an intermediary between the client and the server, but neither the server nor the client can detect its presence. You can add Web proxy support to the SRX Series devices to configure systemwide HTTP connections to the egress traffic to ensure secure communication with the certificate authority (CA) server.

  [See Understanding Certificate Authority Profiles.]

SEE ALSO

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 18.2R1 for the SRX Series.

API and Scripting

- **Junos XML protocol <open-configuration> operation no longer emits an uncommitted changes warning (SRX Series)**—Starting in Junos OS Release 18.2R1, the Junos XML protocol **<open-configuration>** operation does not emit an "**uncommitted changes will be discarded on exit**" warning message when opening a private copy of the candidate configuration. However, Junos OS still discards the uncommitted changes upon closing the private copy.

Application Security

- **Application System Cache for Application Services (SRX Series, vSRX Instances)**—Starting from Junos OS Release 18.2R1, the default behavior of the ASC is changed as following:
  - Security services including security policies, application firewall (AppFW), application tracking (AppTrack), application quality of service (AppQoS), Juniper Sky ATP, IDP, and UTM do not use the ASC by default.
  - Miscellaneous services including advanced policy-based routing (APBR) use the ASC for application identification by default.

    NOTE: The change in the default behavior of the ASC affects the legacy Application Firewall (AppFW) functionality. With the ASC disabled by default for security services starting in Junos OS Release 18.2 onwards, the AppFW will not use the entries present in the ASC.

    You can revert to the ASC behavior as in Junos OS releases prior to 18.2 by using the **set services application-identification application-system-cache security-services** command.

CAUTION: The SRX Series device may become susceptible to application evasion techniques if the ASC is enabled for the security services. We recommend that you enable the ASC only when the performance of the device in its default configuration (disabled for security services) is not sufficient for your specific use case.

Use the following commands to enable or disable the ASC:

- Enable the ASC for security services:

  ```
  user@host# set services application-identification application-system-cache
    security-services
  ```

- Disable the ASC for miscellaneous services:

  ```
  user@host# set services application-identification application-system-cache
    no-miscellaneous-services
  ```

- Disable the enabled ASC for security services:

  ```
  user@host# delete services application-identification application-system-cache
    security-services
  ```

- Enable the disabled ASC for miscellaneous services:

  ```
  user@host# delete services application-identification application-system-cache
    no-miscellaneous-services
  ```

You can use the **show services application-identification application-system-cache** command to verify the status of the ASC.

The following sample output provides the status of the ASC:

user@host>show services application-identification application-system-cache

```
Application System Cache Configurations:
  application-cache: on
    Cache lookup for security-services: off
    Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds
```

For Junos OS Release prior to 18.2R1, application caching is turned on by default. You can manually turn this caching off using the CLI.

```
user@host# set services application-identification no-application-system-cache
```

Attack Detection and Prevention (ADP)

- On SRX1500, SRX4100, SRX4200, and vSRX instances, starting from Junos OS Release 18.2R1, the minimum source-threshold and destination-threshold value range for **tcp syn-flood** is 4~500000. Earlier to this release, the minimum source-threshold and destination-threshold value range for **tcp syn-flood** was 1~500000.

Authentication and Access

- Starting in Junos OS Release 18.2R1, on all SRX Series devices, there must be no space in the password for configuring the Network Time Protocol (NTP) authentication-key. For example **user@host# set system ntp authentication-key 10 type md5 value "ABCDjuniper"**.

  Prior to Junos OS Release 18.2R1, the NTP authentication or password was successfully configured with a space added in the password. For example **user@host# set system ntp authentication-key 10 type md5 value "ABCD juniper"**.

Chassis Cluster

- **IP monitoring**—Starting with Junos OS Release 18.2R1, on all SRX Series devices, if the reth interface is in bundled state, IP monitoring for redundant groups is not supported on the secondary node. This is because the secondary node sends the reply using the lowest port in the bundle that has a different physical MAC address. The reply is not received on the same physical port from which the request is sent. If the reply comes on the other interface of the bundle, then the internal switch drops it.
- **Power entry module**—Starting with Junos OS Release 18.2R1, when you use DC PEM on SRX Series devices operating in chassis cluster mode, the output of **show chassis power** command shows **DC input: 48.0 V input (57000 mV)**. The value **48.0 V input** is a fixed string and can be interpreted as a measured input voltage. The acceptable range of DC input voltage accepted by the DC PEM is 40 to 72 V. The **(57500 mV)** is a measured value, but is not related with the input. It is the actual output value of the PEM and the value is variable. The **DC input:** from **show chassis power** and **Voltage:** information from **show chassis environment pem** command output are removed for each PEM.

Ethernet Switching

- **Interface media access control (MAC) limit** —Starting with Junos OS Release 18.2R1, on SRX4100 and SRX4200 Series devices, the maximum range of MAC addresses configured on the VLAN interface is changed from 1 through 16383 to 1 through 5120. The short description of **interface-mac-limit** at the CLI command hierarchy is changed from **Maximum number of MAC addresses per interface (1..16383)** to **Maximum number of MAC addresses per interface (1..5120)** at the **[edit vlans vlan-name switch-options]** hierarchy level. Prior to Junos OS 18.2R1 Release, if you configure with the 16383 value, commit operation fails during commit.

High Availability (HA) and Resiliency

- **commit fast-synchronize** option not supported for products with single Routing Engine (SRX Series)—Starting in Junos OS Release 18.2R1, Junos OS does not support the configuration option **commit fast-synchronize** at the **[edit system]** hierarchy level for all the products with single Routing Engine for which **chassis redundancy graceful-switchover** is not supported. This option **commit fast-synchronize** is disabled from the CLI.

Interfaces and Chassis

- Support for 802.1p rewrite on **pt** interface (SRX Series)—Starting in Junos OS Release 18.2R1, you can configure 802.1p rewrite on logical VDSL interface, that is, **pt** interface). In previous releases, 802.1p rewrite on VDSL is supported on **ge**, **at**, and other interfaces, except **pt** interface.

IDP

- **Custom Attack (SRX Series)**—Starting with Junos OS Release 18.2R1, the maximum number of characters allowed for a custom attack object name is 60. You can validate the statement using the CLI **set security idp custom-attack** command.

Routing Protocols

- You can configure a designated router (DR) to persist according to your design criteria instead of being subject to the potential vagaries of DR election logic. The **stickydr** feature can prevent traffic loss in a scenario where DR election changes following an interface down event or device upgrade. To enable DR persistence on a configured LAN, enable **stickydr** on all the last hop routers in the LAN.

Security

-

Starting with Junos OS Release 18.2R1, the following commands under the **[edit security utm feature-profile]** hierarchy level are deprecated:

- set web-filtering type
- set web-filtering url-blacklist
- set web-filtering url-whitelist
- set web-filtering http-persist
- set web-filtering http-reassemble
- set web-filtering traceoptions
- set web-filtering juniper-enhanced cache
- set web-filtering juniper-enhanced reputation
- set web-filtering juniper-enhanced query-type
- set anti-virus mime-whitelist
- set anti-virus url-whitelist
- set anti-virus type
- set anti-virus traceoptions
- set anti-virus sophos-engine
- set anti-spam address-blacklist
- set anti-spam address-whitelist
- set anti-spam traceoptions
- set content-filtering traceoptions

[See feature-profile.]

User Interface and Configuration

- **Change to the maximum number of user-defined instances supported by the ephemeral configuration database (SRX Series)**—Starting in Junos OS Release 18.2R1, devices running Junos OS that support configuring the ephemeral configuration database enable configuring a maximum of seven user-defined instances of the ephemeral database. In earlier releases, you can configure up to eight user-defined instances. User-defined instances are configured using the **instance *instance-name*** statement at the **[edit system configuration-database ephemeral]** hierarchy level.
- **Changes to the show ephemeral-configuration command (SRX Series)**—Starting in Junos OS Release 18.2R1, the **show ephemeral-configuration** operational mode command has the following changes:

- To display the configuration data in the default instance of the ephemeral configuration database, issue the **show ephemeral-configuration instance default** command. In earlier releases, ephemeral configuration data for the default instance is displayed using the **show ephemeral-configuration** command.
- To display the configuration data in a user-defined instance of the ephemeral configuration database, issue the **show ephemeral-configuration instance *instance-name*** command. In earlier releases, ephemeral configuration data for a user-defined instance is displayed using the **show ephemeral-configuration *instance-name*** command.
- To view the complete post-inheritance configuration merged with the configuration data in all instances of the ephemeral database, issue the **show ephemeral-configuration merge** command. In earlier releases, the merged view is displayed using the **show ephemeral-configuration | display merge** command.

UTM

- Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the following **show** commands with options **pic** and **fpc** to display physical interface cards (PICs) and Flexible PIC Concentrator (FPC) statistics are deprecated—rather than immediately removed—to provide backward compatibility:
  - **show security utm anti-virus statistics**
  - **show security utm web-filtering statistics**
  - **show security utm content-filtering statistics**
  - **show security utm anti-spam statistics**
  - **show security utm session**
  - **show security utm anti-virus status**
  - **show security utm web-filtering status**

  [See show security utm anti-virus statistics and show security utm web-filtering statistics.]

SEE ALSO

New and Changed Features | 239
Known Behavior | 256
Known Issues | 258
Resolved Issues | 260
Documentation Updates | 264
Migration, Upgrade, and Downgrade Instructions | 265

Product Compatibility | 266

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 18.2R1 for the SRX Series.

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

Chassis Cluster

- On SRX4600 devices, the dedicated chassis cluster fabric ports are not available. Instead, any 40G or 10G traffic ports can be used as chassis cluster fabric ports.
- The SRX5400, SRX5600, and SRX5800 devices operating in a chassis cluster might encounter the em0 or em1 interface link failure on either of the nodes, which results in split-brain condition. That is, both devices are unable to detect each other. If the failure occurs on the secondary node, the secondary node is moved to the disabled state.

  This solution does not cover the following cases:

  - em0 or em1 failure on primary node
  - HA process restart
  - Preempt conditions
  - Control link recovery

Interfaces and Chassis

- On SRX4600 devices, USB disk is not available for the Junos OS. However, the USB disk is available with full access for Host OS (Linux) and USB is still used in the booting process (install and recovery functions). PR1283618
- USB stops working if the USB is removed while it is in initialization state. To avoid this issue, wait for few seconds before removing the USB.PR1332360

J-Web

- On SRX Series devices, DHCP relay configuration under **Configure > Services > DHCP > DHCP Relay** page is removed from J-Web. The same DHCP relay can be configured using the CLI. PR1205911
- On SRX Series devices, DHCP client bindings under Monitor is removed. The same bindings can be seen in CLI using the **show dhcp client binding** command. PR1205915
- On SRX Series devices, adding 2000 global addresses at a time to the SSL proxy profile exempted addresses makes the Web page unresponsive. PR1278087
- On SRX Series devices, you cannot view the custom log files created for event logging in J-Web. PR1280857
- When the UTM policy is detached from the firewall policy rule after an SSL proxy profile is selected, validation is not performed. PR1285543
- Uploading certificate using browse button stores the certificate in device at **/jail/var/tmp/uploads/**, which is deleted when you execute the CLI **request system storage cleanup** command. PR1312529
- The values of address and address-range are not displayed in the inline address-set creation pop-up window of Juniper Identity Management Service (JIMS). PR1312900

Network Management and Monitoring

- An eventd process core file is generated, when the incoming system log message length is at or beyond the maximum supported size of 1024. PR1366120

User Interface and Configuration

- Taking backup of previous configurations takes a long time and causes a delay in committing a configuration with a considerable number of logical system configurations. PR1339862

SEE ALSO

New and Changed Features | **239**

Changes in Behavior and Syntax | **249**

Known Issues | **258**

Resolved Issues | **260**

Documentation Updates | **264**

Migration, Upgrade, and Downgrade Instructions | **265**

Product Compatibility | **266**

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 18.2R1 for the SRX Series.

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

Application Layer Gateways (ALGs)

- In a chassis cluster with logical systems configured, any ALG (except the DNS ALG) enabled, and NAT configured for the ALG sessions, the flowd process on the secondary node might not work. PR1343552

Flow-Based and Packet-Based Processing

- On SRX4100, SRX4200, SRX4600, SRX4800, when dynamic application is configured in security policy core files are observed on the PFE. As a workaround, do not configure dynamic application in security policy. PR1368762
- On SRX Series devices, when a route gets changed, the details are added to the route record module, to update the route record of SRRD module. However, if the last commit time was greater than the route creating time, the rpd process determines that the route record was updated during creation time and hence SRRD will not have the right data against the FIB route. PR1322538

Platform and Infrastructure

- On SRX5600 and SRX5800 devices in a chassis cluster, when a second Routing Engine is installed to enable dual control links, the **show chassis hardware** command shows the same serial number for both the second Routing Engine on both the nodes. PR1321502
- On SRX Series devices in a chassis cluster, configuration commit might succeed even though the external logical interface configuration (reth) associated with the Internet Key Exchange (IKE) VPN gateway configuration is deleted. This might lead to configuration load failure during the next device boot-up. PR1352559
- On SRX4600 devices, the **show chassis fan show chassis environment** command does not display any output. PR1363645

Routing Policy and Firewall Filters

- On SRX Series devices, DNS name entries in policies might not be resolved if the routing instance is configured under a system name server. PR1347006

Routing Protocols

- On SRX Series devices, RIP is supported in packet-to-packet DC mode on st0 interfaces. PR1141817

VPN

- When an SRX Series device acts as an initiator behind the NAT, disabling NAT on the router in between causes an immediate new negotiation failure because of an attempt to disable NAT using the port 4,500.The next attempt succeeds by using the port 500. Disabling NAT and bringing down all the existing tunnels and reestablishing the tunnels with port 500 is the expected behavior. PR1273213
- On SRX Series devices, in case multiple traffic-selectors are configured for a peer with IKEv2 reauthentication, only one traffic-selector will rekey at the time of IKEv2 reauthentication. The VPN tunnels of the remaining traffic selectors will be cleared without immediate rekey. New negotiation of those traffic-selectors might trigger through other mechanisms such as traffic or by peer. PR1287168
- On SRX Series devices, the Policy-based IPsec VPN does not forward traffic correctly when ingress and egress interfaces are in a virtual router. PR1350123
- On SRX Series devices, when using PKI and if there is a dot "." in the configured CA profile name, the pkid process will run into issues after device restart or a PKI service restart, causing PKI-related issues such as CRL download failure. PR1351727

SEE ALSO

New and Changed Features | **239**

Changes in Behavior and Syntax | **249**

Known Behavior | **256**

Resolved Issues | **260**

Documentation Updates | **264**

Migration, Upgrade, and Downgrade Instructions | **265**

Product Compatibility | **266**

Resolved Issues

IN THIS SECTION

This section lists the issues fixed in Junos OS Release 18.2R1 for the SRX Series.

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

Application Layer Gateways (ALGs)

- On SRX Series devices with SIP ALG enabled, the SIP ALG might drop SIP packets that have a **referred-by** or **referred-to header** field containing multiple header parameters. PR1328266
- SIP calls drop when the limit per SPU crosses 10,000 calls. PR1337549

Authentication and Access Control

- On SRX Series devices, the Packet Forwarding Engine might crash and a huge number of core files might be generated within a short time. PR1326677
- On SRX Series devices, incomplete Request Support Information (RSI) might be seen. PR1329967
- On SRX Series devices, the sessions might close because of the **idle Timeout junos-fwauth-adapter** logs. PR1330926
- Web authentication uses hard-coded three seconds timeout but in some scenarios the three seconds timeout is too short to complete a web authentication. Use the new CLI **set access firewall-authentication web-authentication timeout** command to configure web authentication timeout value. PR1339627

Chassis Clustering

- The device might stop forwarding traffic after RG1 failover from node0 to node1. PR1323024
- IP monitoring is not working as expected when one node is in secondary hold state and the primary node's priority is 0. PR1330821

Class of Service (CoS)

- Packets go out of order on SPC2 cards with IOC1 or FIOC cards. PR1339551

Flow-Based and Packet-Based Processing

- On SRX4600 devices, when you execute the **clear security flow session** command, time taken to clear the session depends on the total session number. For example, the clear session takes 9 minutes to clear 57M sessions. PR1308901
- Periodic PIM register loop is observed during switch failure. PR1316428
- The OSPF peers are unable to establish neighbors between the LT interfaces of the logical systems. PR1319859
- The IPv6 traffic does not work as expected on IOC3 with the services offloading (npcache) feature. PR1331401
- SSH to the loopback interface of SRX Series devices does not work properly when AppTrack is configured. PR1343736
- The flowd process might stop when SYN-proxy function is used. PR1343920
- SNMP MIB walk provides incorrect data counters for total current flow sessions. PR1344352
- The interface MAC limit configured under VLANS, which is in the range of the CLI guideline, does not take effect. PR1347245

- File download stops over a period of time when TCP proxy is activated through AV or Juniper Sky ATP PR1349351
- On SRX Series devices in a chassis cluster, if an IPv6 session is being closed and at the same time the related data-plane Redundancy Group (RG1+) failover occurs, this IPv6 session on the backup node might hang and cannot be cleared. PR1354448
- On SRX5000 line devices, when the IPsec performance acceleration feature is enabled, packets going in or out of a VPN tunnel are dropped. PR1357616

Intrusion Detection and Prevention (IDP)

- The control plane CPU usage is high when using IDP. PR1283379
- Loading IDP policy fails due to less available heap memory. PR1347821

J-Web

- J-Web does not display wizards on the dashboard. PR1330283
- When httpd process is not running, J-Web setup wizard does not work after you run the **request system zeroize** command, . PR1335561
- In J-Web you cannot delete dynamic VPN user configuration. PR1348705
- In J-Web menu security policies search button using Internet Explorer version 11 does not work. PR1352910
- The unsupported et and xe interface parameter for speed, link mode, and media type are removed from the **Configure>Interface>Ports** tab in J-Web. PR1355871

Layer 2 Ethernet Services

- The default gateway route might be lost after the failover of RG0 in a chassis cluster. PR1334016

Network Address Translation (NAT)

- Arena utilization on a FPC spikes and then resumes to a normal value. PR1336228

Platform and Infrastructure

- When you perform commits with apply-groups, VPN might flap. PR1242757
- The packet captured by datapath-debug on an IOC2 card might be truncated. PR1300351

- Inconsistent flow-control status on the reth interface is observed. PR1302293
- On SRX5000 line devices using DC PEM, the output of the **show chassis environment pem** and **show chassis power** commands shows incorrect DC input values. PR1323256
- On SRX5400, SRX5600, and SRX5800 devices, SPC2 XLP stops processing packets in the ingress direction after repeated RSI collections. PR1326584
- When Security-Intelligence is configured, IPFD CPU utilization might be higher than expected. PR1326644
- The log messages file contains the **node*.fpc*.pic* Status:1000 from if_np for ifl_copnfig op:2 for ifl :104** message. PR1333380
- Log message **No Port is enabled for FPC# on node0** is generated every 5 seconds. PR1335486
- On SRX4100 devices, interfaces are shown as half-duplex, but there is no impact on the traffic. PR1358066

Routing Policy and Firewall Filters

- Flowd process stops after configuring a huge number of custom applications. PR1347822
- On SRX Series devices, a large-scale commit, for example, a 70,000-lines security policy, might stop the nsd process on the Packet Forwarding Engine. PR1354576

Routing Protocols

- When BGP traceoptions are configured and enabled, the traces specific to messages sent to the BGP peer (BGP SEND traces) are not logged The traces specific to received messages (BGP RECV traces) are logged correctly. PR1318830
- On SRX Series devices, dedicated BFD does not work. PR1347662

Unified Threat Management (UTM)

- The ISSU upgrade might fail due to the Packet Forwarding Engine generating a core file. PR1328665

VLAN Infrastructure

- On SRX Series devices in transparent mode, the flowd process might stop when matching the destination MAC. PR1355381

VPN

- IPsec traffic statistic counters return 32-bit values. PR1301688
- PKID syslog for key-pair deletion is required for conformance. PR1308364
- SNMP for jnxIpSecTunMonVpnName does not work. PR1330365
- The kmd process might generate core files when all VPNs are down. PR1336368
- All IPsec tunnels are in both active and inactive state. PR1348767
- S2S tunnels are not redistributed after IKE and IPsec are reactivated in a configuration. PR1354440

SEE ALSO

New and Changed Features | 239

Changes in Behavior and Syntax | 249

Known Behavior | 256

Known Issues | 258

Documentation Updates | 264

Migration, Upgrade, and Downgrade Instructions | 265

Product Compatibility | 266

Documentation Updates

There are no errata or changes in Junos OS Release 18.2R1 documentation for the SRX Series.

SEE ALSO

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 might occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 15.1X49, 17.3, 17.4, 18.1 and 18.2 are EEOL releases. You can upgrade from one Junos OS Release to the next release or one release after the next release. For example you can upgrade from Junos OS Release 15.1X49 to Release 17.3 or 17.4, Junos OS Release 17.4 to Release 18.1 or 18.2, and from Junos OS Release 18.1 to Release 18.2 or 18.3 and so on.

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

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

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

For information about ISSU, see the Chassis Cluster User Guide for Security Devices.

SEE ALSO

New and Changed Features | 239
Changes in Behavior and Syntax | 249
Known Behavior | 256
Known Issues | 258
Resolved Issues | 260
Documentation Updates | 264
Product Compatibility | 266

Product Compatibility

Hardware Compatibility

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

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

Find Feature Explorer at: https://pathfinder.juniper.net/feature-explorer/

SEE ALSO

New and Changed Features | 239
Changes in Behavior and Syntax | 249
Known Behavior | 256
Known Issues | 258
Resolved Issues | 260
Documentation Updates | 264
Migration, Upgrade, and Downgrade Instructions | 265

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.

Compliance Advisor

For regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6 for Juniper Networks products, see the Juniper Networks Compliance Advisor.

Finding More Information

For the latest, most complete information about known and resolved issues with the Junos OS, see the Juniper Networks Problem Report Search application at https://prsearch.juniper.net.

For regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6 for Juniper Networks products, see the Juniper Networks Compliance Advisor.

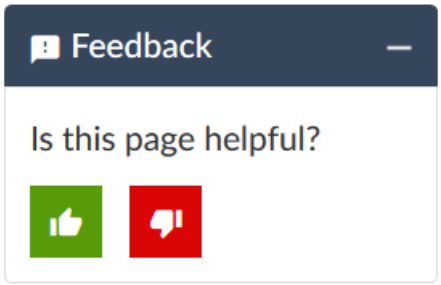
To access Software Release Notifications for Junos OS Service Releases, visit our Knowledge Center at https://support.juniper.net/support/. You'll need to log in to your Juniper Account. From the Knowledge Center, search by the specific release number, for example 17.4R1-S2. Use the Software Release Notifications to download software, and learn about known and resolved issues for specific service releases.

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at https://apps.juniper.net/feature-explorer/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies— For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties— For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC Hours of Operation — The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://support.juniper.net/support/
- Search for known bugs: https://kb.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://support.juniper.net/support/downloads/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://forums.juniper.net/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) tool located at https://entitlementsearch.juniper.net/entitlementsearch/ .

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at https://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at https://www.juniper.net/support/requesting-support.html.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net/pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to support@juniper.net. For documentation issues, fill out the bug report form located at https://www.juniper.net/cgi-bin/docbugreport/.

Revision History

26 August 2021—Revision 29, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

17 June 2021—Revision 28, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

05 February 2021—Revision 27, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

26 March 2020—Revision 26, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

11 October 2019—Revision 25, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

5 September 2019—Revision 24, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

8 August 2019—Revision 23, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

18 July 2019—Revision 22, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

11 April 2019—Revision 21, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

4 April 2019—Revision 20, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

14 March 2019—Revision 19, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

28 February 2019—Revision 18, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

14 February 2019—Revision 17, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

11 December 2018—Revision 16, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

29 November 2018—Revision 15, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

15 November 2018—Revision 14, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

31 October 2018—Revision 13, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

25 October 2018—Revision 12, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

20 September 2018—Revision 11, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

18 September 2018—Revision 10, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

6 September 2018—Revision 9, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

29 August 2018—Revision 8, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

21 August 2018—Revision 7, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

15 August 2018—Revision 6, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

10 August 2018—Revision 5, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

2 August 2018—Revision 4, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

19 July 2018—Revision 3, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

6 July 2018—Revision 2, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

29 June 2018—Revision 1, Junos OS Release 18.2R1– ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.