Release Notes

Junos OS Evolved Release 22.3R1

HARDWARE HIGHLIGHTS

- New ACX7024 router

Introduction

Use these release notes to find new and updated features, software limitations, and open issues for Junos OS Evolved Release 22.3R1.

For more information on this release of Junos OS Evolved, see Introducing Junos OS Evolved.

JUNIPer
NETWORKS | Engineering
Simplicity

Table of Contents

Key Features in Junos OS Evolved Release 22.3

Start here to learn about the key features in Junos OS Evolved Release 22.3. For more information about a feature, click the link in the feature description.

- **Limited image version support of Junos OS Evolved** (ACX7509)

  This limited image does not have data-plane encryption and is intended only for the countries of the Eurasian Customs Union (EACU). These countries have import restrictions on software containing data-plane encryption.

  [See Junos OS Evolved Installation Packages.]

- **Priority-based flow control X-ON Threshold and per-queue alpha support (QFX5220)**—The priority-based flow control (PFC) X-ON threshold is the ingress port's priority group (PG) shared buffer limit. At this limit, the ingress port's peer resumes transmission of packets after a brief PAUSE because of the PFC message sent by this ingress port. You can tune globally the limit of buffers that each queue can consume from the shared pool based on the dynamic threshold setting called the *alpha value*. Starting with Junos OS Evolved 22.3R1 on QFX5220 devices, you can fine tune the X-ON threshold through the congestion notification profile (CNP) and fine tune the alpha value on a per-queue basis through a scheduler.

  [See xon (Input Congestion Notification) and buffer-dynamic-threshold .]

- **Synchronous Ethernet with G.8262 Standard Support (ACX7509)**—Starting in Junos OS Evolved Release 22.3R1, ACX7509 routers support Synchronous Ethernet features compliant with the following International Telecommunication Union Telecommunication Standardization (ITU-T) standards to facilitate the transference of clock signals over the Ethernet physical layer.

  - Synchronous Ethernet (G.8262) – Timing and synchronization aspects in packet networks. Specifies timing characteristics of synchronous Ethernet equipment clock (EEC).

  - Synchronous Ethernet Enhanced (G.8262.1)

  [See Synchronous Ethernet.]

- **Telemetry support for CoS ingress packet drop accounting (QFX5220)**—Junos OS Evolved Release 22.3R1 introduces telemetry support to account for packets that are dropped because of ingress port congestion. Counters for priority flow control (PFC), explicit congestion notification (ECN), and ingress drops are exported using the sensor **/junos/system/linecard/interface/traffic**. Counters for PFC, ECN, and ingress drops are also exported using OpenConfig sensor **/interfaces/interface/**. Priority group (PG) buffer utilization is exported using the sensor **/junos/system/linecard/qmon-sw/**.

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

Junos OS Evolved Release Notes for ACX7024, ACX7100-32C, ACX7100-48L, and ACX7509 Devices

IN THIS SECTION

These release notes accompany Junos OS Evolved Release 22.3R1 for ACX7024, ACX7100-32C, ACX7100-48L, and ACX7509 devices. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

What's New

IN THIS SECTION

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

To view features supported on the ACX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Evolved Release 22.3R1, click the Group by Release link. You can collapse and expand the list as needed.

- ACX7024

- ACX7100-32C

- ACX7100-48L

- ACX7509

The following sections highlight the key features in this release.

Hardware

- **New ACX7024 router (ACX Series)**—Starting in Junos OS Evolved Release 22.3R1, we introduce the Juniper Networks ACX7024 Cloud Metro Router, a high-performance access router that meets the growing demands of metro applications. With a compact 1-U form factor, temperature-hardened design, and advanced timing features, the ACX7024 supports Ethernet business services, residential access, and 5G mobile deployments. The ACX7024 also supports the latest protocol and traffic engineering technologies and offers a tamper-proof design that ensures strong security capabilities.

  The ACX7024 router provides a switching capacity of 360 Gbps and the following port configurations:

  - Four 100-Gigabit Ethernet (GbE) ports (ports 0 through 3) that support quad small form-factor pluggable 28 (QSFP28) transceivers. You can channelize these ports into four 25-Gbps interfaces using breakout cables (and channelization configuration). These ports also support 40-Gbps speed when you use QSFP+ optics. You can channelize these 40-Gbps ports into four 10-Gbps interfaces using breakout cables (and channelization configuration).

  - Twenty-four 25-GbE ports (ports 4 through 27) that operate at 25-Gbps speed with SFP28 transceivers, 10-Gbps speed with SFP+ transceivers, or 1-Gbps speed with SFP transceivers.

You can order the routers with front-to-back airflow (airflow out or AFO) and with AC or DC power supply modules (PSMs).

Table 1: Features Supported on the ACX7024 Router

Feature	Description
Chassis	- Support for environmental monitoring and field-replaceable unit (FRU) management. [See show chassis hardware.] - Support for Single power supply module (PSM) and PSM Redundancy—The ACX7024 router supports dual PSM (1+1 redundancy) mode by default, and also single PSM mode. Use the `set chassis pem minimum <number>` command to configure single PSM and set it to 1. [See pem (M320, ACX7024 Devices), show chassis power.]
Class of Service	- Support for classification and rewrite rules of all types (Inet-Prec, DSCP, DSCPv6, IEEE-802.1p, IEEE-802.1ad) at the logical interface level. [See Classifiers and Rewrite Rules at the Global, Physical, and Logical Interface Levels Overview.] - Logical interfaces support classification and rewrite rules for MPLS, VPLS, L3VPN, L2CKT, CCC, IRB, and EVPN. [See Classifiers and Rewrite Rules at the Global, Physical, and Logical Interface Levels Overview.] - The ACX7024 supports deep buffering of oversubscribed traffic and absorbs network bursts, as follows: - The router buffers packets using on-chip SRAM and external high-bandwidth memory (HBM). - On-chip buffer (OCB) size is 8MB and HMB size is 2GB. - The default delay buffer size per port is 100 us. - The router absorbs bursts up to 20 ms of buffer per port. This feature is enabled by default. [See Shared and Dedicated Buffer Memory Pools on ACX Series Routers.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
DHCP	• DHCP server and DHCP relay configuration for IPv4 and IPv6 services. [See DHCP Overview.]
Ethernet Protocols	• Support for Ethernet ring protection switching (ERPS) with G.8032 version 2. [See Understanding Ethernet Ring Protection Switching Functionality.] • Support for Layer 2 Protocol Tunneling (L2PT)—You can use L2PT to send L2 protocol data units (PDUs) across the network and deliver them to devices that are not part of the local broadcast domain. You can configure L2PT using the `protocol <protocol name>` configuration statement at the [`edit protocols layer2-control mac-rewrite interface <interface name>`] hierarchy level and destination MAC address using the `tunnel-destination-mac <mac address>` configuration statement at the [`edit protocols layer2-control mac-rewrite`] hierarchy level. • Support for Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP). [See Spanning-Tree Protocol Overview.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description

EVPN	• Support for EVPN-MPLS—ACX7024 router supports the following EVPN-MPLS features on MAC-VRF instances:
	
	   • L2 flooding for broadcast, unknown unicast, and multicast (BUM) traffic
	
	   • Split-horizon between core interfaces
	
	   • Data plane and control plane MAC learning and aging, and static MAC
	
	   • MAC movement and MAC mobility on control plane only
	
	   • MAC limiting and MAC learning
	
	   • Input and output VLAN maps using normalization on user-to-network interfaces (UNIs)
	
	   • Aggregated Ethernet interfaces used for UNIs and network node interfaces (NNIs)
	
	   • Physical interfaces for VLAN tagging, stacked VLAN tagging, flexible VLAN tagging, and extended VLAN bridges using EVPN-MPLS as a service
	
	   • Ethernet bridge mode for logical UNIs
	
	   • VLAN ID lists, native VLAN ID supported logical UNIs, and priority-tagged logical interfaces
	
	   • Underlay with ECMP and Fast reroute (FRR)
	
	   • Control-word support for EVPN
	
	   • EVPN Proxy Address Resolution Protocol (ARP) and ARP suppression
	
	  [See EVPN Feature Guide.]
	
	• Virtual private wire service (VPWS) with EVPN signaling mechanisms and flexible cross-connect support.
	
	  [See Overview of VPWS with EVPN Signaling Mechanisms.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
Firewall Filters	• Support for firewall filters and policers—ACX7024 router supports configuring firewall filters with packet match conditions for the following families: bridge domain, IPv4, IPv6, CCC, and MPLS. In addition to packet match conditions, the following actions are supported: count, discard, log, syslog, and policer. [See Standard Firewall Filter Match Conditions and Actions on ACX Series Routers Overview.] • Firewall filter protocols: MPLS, CCC, virtual private LAN service (VPLS), and ANY. [See Firewall Filters Overview.]

High Availability	• Support for the following Bidirectional Forwarding Detection (BFD) features:
	
	  • BFD for IPv4 and IPv6 routes
	
	  • Single-hop BFD in inline mode with an interval range of 4 milliseconds to 1 second
	
	  • Single-hop BFD in distributed mode with an interval of 1 second or more
	
	  • Single-hop BFD in centralized mode with a minimum interval of 1 second to detect IRB failures
	
	  • Multihop BFD with an interval of 1 second or more
	
	  • Micro-BFD for LAG in centralized or distributed mode with an interval of 1 second or more
	
	[See Bidirectional Forwarding Detection (BFD).]
	
	• You can configure BFD over label-switched paths (LSPs) or RSVP-based LSPs in a centralized mode. [See Bidirectional Forwarding Detection (BFD) for MPLS.]
	
	• VRRP for IPv4 and IPv6. [See VRRP and VRRP for IPv6 Overview.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
Interfaces	• Support for 1RU Metro Ethernet device —The ACX7024 router is a high-density 1RU Metro Ethernet device with 28 ports. You can configure the first four ports as 40-Gigabit or 100-Gigabit Ethernet interfaces. The first four ports also support channelization. Ports 0-3 also supports 10-Gigabit and 25-Gigabit Ethernet interfaces using channelization. You can configure the remaining 24 ports as 1-Gigabit, 10-Gigabit, or 25-Gigabit Ethernet interfaces. By default, the ports are 10-Gigabit and 100-Gigabit Ethernet interfaces. **NOTE**: If you enable PTP mode, the system deletes port et-0/0/27. To configure the port speed of the line card, use the statement at the [set interfaces <intf name> speed <speed>] hierarchy. Assign the speed value as <1G | 10G | 25G | 40G | 100G >. To disable the port, use the set interfaces <intf name> unused command. [See Port Speed.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description

Layer 2 features	• Support for the following advanced L2 features:
	
	  • 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
	
	  • Single-learning domain
	
	  • MAC limiting
	
	  • Ethernet service types:
	
	    • E-Line with these AC interface types: port, VLAN, Q-in-Q, VLAN list, and VLAN maps
	
	    • E-line
	
	    • E-LAN
	
	    • E-Access
	
	    • E-Transit
	
	  • LLDP
	
	  • LACP
	
	  • IRB interface
	
	  • Link aggregation group (LAG) support with the following hashing algorithms:
	
	    • For family `multiservice`, destination and source MAC addresses
	
	    • For family `inet`, Layer 3 and Layer 4

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
	- For family `inet6`, Layer 3 destination and source addresses - For family `inet6`, Layer 4 destination and source ports - Encapsulation types: `extended-vlan-bridge` `vlan-bridge` - Q-in-Q tunneling [See Understanding Layer 2 Bridge Domains and Q-in-Q Tunneling.] - Disable local switching in bridge domains. [See Configuring MAC Address Flooding and Learning for VPLS.] - Storm control [See Understanding Storm Control.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description

Layer 2 VPN	• Support for VPLS—The ACX7024 routers support a single VLAN for each virtual switch routing instance type. Junos OS Evolved does not support the family vpls option. To configure VPLS on the ACX7024 routers, configure the instance-type virtual switch statement at the [edit routing-instances routing instance] hierarchy level.
	
	[See Introduction to Configuring VPLS.]
	
	• Layer 2 VPN and L2 circuit support:
	
	    • L2 circuit—Targeted LDP signaling pseudowires and interoperability between different types of supported attachment circuit (AC) for L2 circuit
	
	    • L2 VPN circuit—BGP signaling
	
	• MPLS fast reroute (FRR) on IGP, circuit attachment types (port, VLAN, and Q-in-Q tunneling), control word, pseudowire circuit on aggregated Ethernet interfaces, indirect next hops and composite next hops, pipe and uniform mode time-to-live (TTL), Tag Protocol Identifiers (TPIDs), and VLAN map on pop, push, or swap
	
	[See Understanding Layer 2 VPNs and Understanding Layer 2 VPNs and Configuring Interfaces for Layer 2 Circuits.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description

Layer 3 features	• Support for the following Layer 3 features:
	
	  • Longest prefix match
	
	  • Exception packets handling
	
	  • VLAN tagging modes
	
	  • Neighbor solicitation
	
	  • Unicast RPF
	
	  • Interface-based routing
	
	  • Integrated routing and bridging (IRB)
	
	The ACX7024 router also supports interior gateway protocols such as OSPF, IS-IS, RIP, and ECMP. [See Configure ICMP Features, Enabling VLAN Tagging, Neighbor solicitation, Understanding Unicast RPF (Routers), OSPF Overview, IS-IS Overview, and RIP User Guide.]
	
	• Support for BGP for IPv4 and IPv6. [See BGP Overview.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description

Layer 3 VPN	• Support for the following Layer 3 (L3) VPN features:
	
	  • IP-VPN services:
	
	    • Virtual routing and forwarding (VRF) and virtual-router instance type
	
	    • All control plane configuration options
	
	    • Per-prefix and per-table label signaling
	
	    • L3 VPN support with ECMP
	
	    • BGP policies support for different L3 VPN use cases such as full mesh VPN, hub-spoke VPN, management VPN, and leaking routes
	
	    • L3 VPN with `vrf-table-label` mode
	
	    • L3 VPN with `chained-composite-next-hop` mode
	
	    • L3 VPN ping using `ping mpls l3vpn prefix prefix-name l3vpn` *name* command
	
	      NOTE: The ping command works only with the `vrf-table-label` configuration.
	
	  • 6PE and 6VPE with PE-CE routing-static and PE-to-CE BGPv6
	
	  • Import and export of routes across non-default to non-default virtual routing and forwarding (VRF)
	
	    NOTE: Table next hop is not supported.
	
	  • Inter-autonomous system (Inter-AS) options A, B, and C
	
	    NOTE: You can deploy inter-AS option B in a hierarchical network design within a single interior gateway protocol (IGP) autonomous system.

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
	• Provider edge-to-customer edge (PE-to-CE) route using static route and routing protocols such as eBGP, IS-IS, OSPF, and RIP Currently, we do not support virtual tunnel (VT) interface-based L3 VPN. [See Layer 3 VPNs User Guide for Routing Devices.]
Management	• Support for NETCONF, Transport Layer Security (TLS), YANG, and OpenConfig management features.

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
MPLS	- Support for the following MPLS features: - IP/MPLS infrastructure feature set for the L3 VPN service - Basic BGP control plane features such as LDP-DOD, CSPF, and single-area CSPF - MPLS label stack - MPLS protections: - Fast reroute (FRR)/ Make-before-break (MBB) - Link protection - Node protection - Label-switching router (LSR) - Shared Risk Link Group (SRLG) for MPLS - RSVP label-switched path (LSP) over IPv4 include refresh reduction - Label Distribution Protocol (LDP) LSP over IPv4 - RSVP 1:1 - RSVP-Traffic Engineering (RSVP-TE) - LDP over RSVP - Inter-autonomous system LSP intra-area LSP [See MPLS Applications User Guide.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
Multicast	- Support for L2 multicast-related features, includes Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) snooping. You can configure IGMP snooping with IGMPv1, IGMPv2, and IGMPv3, which includes the support for: - IGMP snooping in Bridge Domain (BD) - IGMP snooping with integrated routing and bridging (IRB) configured in BD - MLD snooping in BD - MLD snooping with IRB configured in BD [See IGMP Snooping Overview and Understanding MLD Snooping.] - Support for IPv4 multicast for L3. You can configure IGMP snooping with IGMPv2 and IGMPv3, which includes support for the following: - Auto-rendezvous point (auto-RP) - Anycast RP - IGMP filter - IGMP querier - Protocol Independent Multicast source-specific multicast (PIM SSM) - PIM sparse mode (PIM SM) **NOTE**: In this Junos OS Evolved release, the ACX7024 doesn't support IPv6 multicast or L3 multicast protocols (such as IGMP, MLD, or PIM) over IPv4 and IPv6 IRB interfaces. [See IGMP Snooping Overview.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
	- Support for multichassis link aggregation groups (MC-LAGs). The following features are available on MC-LAGs: - Layer 2 bridging for active-active and active-standby modes - Layer 3 unicast [See Understanding Multichassis Link Aggregation Groups.]
Operations, Administration, and Management	- Support for Operations, Administration, and Management (OAM). You can configure the connectivity fault management (CFM), BFD, ITU-T Y.1731 standard for Ethernet service OAM. You can also configure the following features of link-fault management (LFM): - Discovery - Link monitoring - Remote fault detection [See ITU-T Y.1731 Ethernet Service OAM Overview and Introduction to OAM Link Fault Management (LFM).] - Support for IEEE 802.1ag OAM CFM. - Support for IEEE Standard 802.3ah and 802.1ag for OAM CFM DOWN and UP maintenance association end points (MEPs) over virtual private LAN service (VPLS) - Support for IEEE Standard 802.3ah and 802.1ag for OAM CFM UP maintenance association end points (MEPs) over EVPN [See IEEE 802.3ah OAM Link-Fault Management Overview and IEEE 802.1ag OAM Connectivity Fault Management Overview.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
Resiliency	Support for platform resiliency to handle failures and faults related to components such as CPU, fan trays, temperature sensors, power supply units, FPGA, and optics. Fault handling includes detecting and logging the error, raising alarms, sending SNMP traps, communicating errors through LEDs, self-healing, and taking components out of service. [See show system errors active.]
Routing Policy	Unicast reverse path forwarding (unicast RPF) support for IPv4 and IPv6. You can reduce the impact of denial-of-service (DoS) attacks for IPv4 and IPv6 interfaces by configuring unicast RPF. You can use unicast RPF to determine the source of attacks and reject packets from unexpected source addresses on interfaces. However, we do not support unicast RPF checking for: • Transit packets exiting a tunnel source interface. • Asymmetrical routing. [See Understanding Unicast RPF (Routers).]
Segment Routing	Support for segment routing—The following segment routing features are supported: • Segment routing global block (SRGB) for OSPF and IS-IS • Fast reroute • Metro Ethernet services over segment routing infrastructure

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
	Support for segment routing—The following segment routing features are supported: • Segment routing services: L3VPN, IPv6 VPN Provider Edge (6VPE) , IPv6 Provider Edge (6PE), Layer 2 (L2) VPN, L2 Circuit, and BGP-VPLS • Static segment routing (node segment, prefix segment, adjacency, and anycast segments) for OSPF and IS-IS • Topology-independent loop-free alternate (TI-LFA) with segment routing for OSPF and IS-IS [See Understanding Topology-Independent Loop-Free Alternate with Segment Routing for IS-IS, Understanding Source Packet Routing in Networking (SPRING), and Understanding Adjacency Segments, Anycast Segments, and Configurable SRGB in SPRING.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
Services applications	• Support for RFC 5357, Two-Way Active Measurement Protocol (TWAMP) monitoring service. You can configure the TWAMP monitoring service, which sends out probes to measure network performance. You often use TWAMP to check compliance with service-level agreements. In Junos OS Evolved, you configure TWAMP at the [edit services monitoring twamp] hierarchy level. The support for this service is limited to the following: • IPv4 traffic only for control sessions and test sessions • Probe statistics and history • Control and test session status • Test session probe generation and reception, as well as reflection • Timestamps set by the Routing Engine or the Packet Forwarding Engine • Error reporting through system log messages only • Unauthenticated mode only • TWAMP IPv6 address support—You can specify IPv6 source and target addresses for TWAMP clients, control connections, and test sessions. [See Understanding Two-Way Active Measurement Protocol on Routers.]

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
Software installation and upgrade	• Support for secure-boot implementation based on the UEFI 2.4 standard. [See Secure Boot.] • Support for either WAN interfaces or management interfaces to automatically download and install the appropriate software and the configuration file on your device during the ZTP bootstrap process. [See Zero Touch Provisioning.]
Security Services	• Support for distributed denial of service (DDoS) protection, which is enabled by default. [See Control Plane Distributed Denial-of-Service (DDoS) Protection Overview.]
System Management	• Support for an alternate partition for device recovery—An alternate partition called /altconfig is used to recover the device when the /config partition gets corrupted. In certain scenarios, the /config (which holds the last four committed configuration files along with the rescue configuration) gets corrupted during resets or power cycles. The /altconfig partition (which holds the juniper.conf.gz and rescue.conf.gz files) is used by the management daemon (mgd) to recover the device when the /config is corrupted. This is a boot time feature and is enabled by default.

Table 1: Features Supported on the ACX7024 Router *(Continued)*

Feature	Description
Timing and synchronization	- Support for enhanced Ethernet equipment clock (eEEC). Enhanced EEC enables new clocks to operate with different quality levels defined in the Synchronous Ethernet chain. To enable enhanced EEC on your router, configure the `enable-extended-qltlv` statement at the `[edit chassis synchronization]` hierarchy level. The ACX7024 supports the following new clock quality levels for enhanced EEC: - Enhanced primary reference time clock (ePRTC) - Primary reference time clock (PRTC) - Enhanced primary reference clock (ePRC - Enhanced Ethernet equipment clock (eEEC) [See enable-extended-ql-tlv, Ethernet Synchronization Message Channel Overview, and synchronization.] - Support for frequency synchronization using Synchronous Ethernet. [See Synchronous Ethernet Overview.] - Support for G.8275.1 telecom profile, Precision Time Protocol (PTP) over Ethernet encapsulation, and hybrid mode. [See Precision Time Protocol Overview and Understanding Hybrid Mode.] - Support for Precision Time Protocol (PTP) G.8275.1 enh and G.8275.2 enh profiles with PTP over IPv4 and IPv6 unicast. The G.8275.1 enh profile does not support unicast negotiation. [See PTP profiles.]

To view the hardware compatibility matrix for optical interfaces, transceivers, and DACs supported on the ACX7024 router, see the Hardware Compatibility Tool.

Class of Service

- **Hierarchical Class of Service (CoS) support (ACX7024, ACX7100-32C, ACX7100-48L, and ACX7509)**
—Starting with Junos OS Evolved 22.3R1, ACX routers that run Junos OS Evolved support

hierarchical CoS. By enabling hierarchical scheduling, an ACX interface running Junos OS Evolved can support three levels of scheduling (physical interfaces, logical interfaces, and queues). ACX routers running Junos OS Evolved do not support hierarchical CoS on integrated bridging and routing (IRB) or aggregated Ethernet interfaces. Also, hierarchical CoS schedulers should not include buffer or drop profile configurations.

To enable hierarchical scheduling, set `hierarchical-scheduler` at the `[edit interfaces` *interface-name* hierarchy level.

[See Hierarchical Class of Service in ACX Series Routers.]

EVPN

- **Remote port mirroring with an IP address (GRE encapsulation) on EVPN-VXLAN (ACX7100-32C and ACX7100-48L)**—Starting in Junos OS Evolved 22.3R1, you can configure remote port mirroring with an IP address on an EVPN-VXLAN fabric. The router sends the mirrored traffic output through a GRE tunnel to the remote IP destination address that you specify in the configuration. The configuration is an analyzer instance.

    > **(i) NOTE**: Configure the feature under the `[edit forwarding-options analyzer]` hierarchy level. You cannot configure it under `[edit forwarding-options port-mirroring]`.

    Configuration guidelines include:

    - You can configure a nonzero logical unit number for an input analyzer; however, the chip in an ACX7100 router supports mirroring in the hardware on the physical interface, not on a logical interface.

    - In ingress mirroring, incoming traffic is mirrored at the ingress pipeline, and therefore pruning or filtering at the egress pipeline does not have any impact on the mirroring behavior.

    - Input families for the input port are `inet`, `inet6`, `ethernet-switching`, and `bridge`.

    - The destination address for mirrored output must be an IPv4 address.

    [See Port Mirroring and Analyzers.]

- **Support for EVPN ELAN active-active multihoming and EVPN over segment routing (ACX7024)**—Starting in Junos OS Evolved Release 22.3R1, we support the following EVPN segment routing features:

    - EVPN-ELAN active-active multihoming

    - EVPN-ELAN over segment routing

        - Segment routing global block (SRGB) for OSPF and IS-IS

- Segment routing services for IPv4

- Metro Ethernet services over segment routing infrastructure

- Static segment routing (node segment)

- MPLS fast reroute

- Topology-independent loop-free alternate (TI-LFA) with segment routing for OSPF and IS-IS

[See EVPN Multihoming Overview and Example: Configuring EVPN Active-Active Multihoming.

- **Support for all-active multihoming redundancy in FXC and non-FXC EVPN-VPWS networks (ACX7024)**—Starting in Junos OS Evolved Release 22.3R1, you can configure an ACX7024 device in both types of EVPN–virtual private wire service (EVPN-VPWS) network with flexible cross-connect (FXC) or legacy EVPN-VPWS (non-FXC) networks to support all-active multihoming redundancy.

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

- **Support for EVPN-VPWS all-active multihoming for segment routing over MPLS (ACX7024)**—Starting in Junos OS Evolved Release 22.3R1, we support two variants of EVPN-VPWS multihoming for segment routing over MPLS: all-active and single-active. All-active instances share traffic to each multihomed provider edge. The single-active instances are cold-standby acting as single-homed models where the routing protocol daemon (RPD) is aware of the backup path. If the primary path goes down, the Packet Forwarding Engine (PFE) is updated with the new path. This release supports up to 512 instances of multihomed neighbors. Note that this release does not support asynchronous notification.

  [See Overview of VPWS with EVPN Signaling Mechanisms.]

Forwarding Options

- **Firewall filter actions (ACX7024)**—Starting in Junos OS Evolved 22.3R1, we support the following firewall filter actions to configure filter-based forwarding or policy-based forwarding.

  - next-ip firewall filter action for IPv4 address

  - next-ip6 firewall filter action for IPv6 address

  - next-interface firewall filter action for an interface

  [See Filter-Based Forwarding Overview and Understanding Filter-Based Forwarding to a Specific Outgoing Interface or Destination IP Address.]

Junos Telemetry Interface

- **BGP policy sensor upgrade (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Release 22.3R1, JTI supports data

model **openconfig-bgp-policy.yang** version 6.0.2 (upgraded from version 4.0.1). New BGP policy sensors are supported.

[See Telemetry Sensor Explorer.]

- **MPLS RSVP-TE sensor support (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos Evolved OS Release 22.3R1, Junos telemetry interface (JTI) supports the data model **openconfig-mpls-rsvp.yang** version 4.0.0. It also supports the new RSVP-Traffic Engineering (RSVP-TE) sensors.

  [See Telemetry Sensor Explorer.]

- **MPLS OpenConfig configuration and sensor support (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 22.3R1, Junos telemetry interface (JTI) supports these data models:

  - **openconfig-mpls.yang** version 3.2.2

  - **openconfig-mpls-types.yang** version 3.2.1

  - **openconfig-mpls-te.yang** version 3.2.2

  - **openconfig-mpls-static.yang** version 3.2.2

  The release supports these OpenConfig configurations:

  - MPLS global

  - MPLS named-explicit-path

  - MPLS tunnels

  The release supports these state groups:

  - MPLS tunnels

  - MPLS named-explicit-path

  - MPLS static label-switched-path

  - MPLS-TE interface attributes

  - MPLS tunnel state counters (dependent on the Packet Forwarding Engine)

  [See Telemetry Sensor Explorer and Mapping OpenConfig MPLS Commands to Junos Configuration.]

- **Platform sensor support for components, optics, physical interfaces, and Ethernet interfaces (ACX7100-32C, and ACX7100-48L, and ACX7024)**—Starting in Junos OS Evolved Release 22.3R1, Junos telemetry interface (JTI) supports sensors for components, optics, physical interfaces, and Ethernet interfaces.

For optics sensors, see Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface). For other sensors, see Telemetry Sensor Explorer.]

Layer 2 VPN

- **Support for Redundant Pseudowires for Virtual Private LAN Service (VPLS) (ACX7024)**—Starting in Junos OS Evolved 22.3R1, VPLS with LDP hot-standby, cold-standby model, and without BFD or CFM trigger is supported.

   [See Redundant Pseudowires for Layer 2 Circuits and VPLS.]

- **Support for Redundant Pseudowire Layer 2 Circuits (ACX7024)**—Starting in Junos OS Evolved 22.3R1, ACX7024 supports redundant pseudowire Layer 2 Circuits. Multichassis Link Aggregation Group (MC-LAG) is not supported with redundant pseudowire Layer 2 circuits.

   [See Redundant Pseudowires for Layer 2 Circuits and VPLS.]

- **Flow-Aware Transport for Pseudowires (FAT) label and Entropy label support for Layer 2 circuit and Layer 2 VPN (ACX7024)**—Starting in Junos OS Evolved 22.3R1, VPLS with LDP hot-standby, cold-standby model, and without BFD or CFM trigger is supported.

   FAT Label support includes these features:

   - Transmit and receive direction on Layer 2 circuits and Layer 2 VPNs

   - Transmit and receive direction on Layer 2 VPN

   - Layer 2 VPN with multihoming

   - Layer 2 circuits with redundant pseudowire

   - Load balancing over LAG

   - Static flow label for Layer 2 circuits

   Entropy Label support includes these features:

   - Entropy label indication for LDP and RSVP transport

   - Load balancing over LAG

   [See FAT Flow Labels Overview and Configuring Entropy Labels .]

OpenConfig

- **OpenConfig BFD configuration and state support (ACX7100-32C, ACX7100-48L, PTX10001-36MR, PTX10003, PTX10008, and PTX10016)**—Junos OS Evolved Release 22.3R1 introduces OpenConfig configuration support and state support for Birdirectional Forwarding Detection (BFD).

[See Mapping OpenConfig Interface Commands to Junos Configuration and Telemetry Sensor Explorer.]

Precision Time Protocol (PTP)

- **Support for Synchronous Ethernet with Precision Time Protocol (PTP) Transparent Clock (ACX7024)**—The transparent clock measures the residence time of PTP packets as the packets pass through the router. The network load and device architecture might result in queuing or buffering delays. These delays are the main source of packet delay variation in the router.

  Transparent clock adds the residence time into the correction field of the PTP packet. The client or boundary clocks can determine this resident time while they receive the PTP packet from the upstream transparent clock router. The client clock can estimate and remove these delays from the offset computation and reduce the packet's jitter effects.

  In a syntonized transparent clock, the transparent clock requires physical layer frequency based on the ITU-T G.8262/.1 standard. Synchronous Ethernet configuration is mandatory for enabling a syntonized transparent clock.

  Use the `show protocols ptp` and `show ptp global-information` commands to verify the PTP transparent clock configuration status.

  To enable PTP transparent clock on your device, configure the `syntonized-e2e-transparent` configuration statement at the [`edit protocols ptp`] hierarchy level.

  [See PTP Transparent Clocks and show ptp global-information.]

Routing Protocols

- **Maximum reference bandwidth increased to 4 TB for IGP protocols (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016, QFX5130-32CD, QFX5700, and QFX5220)**—Starting with Junos OS Evolved Release 22.3R1, we've increased the maximum reference bandwidth for IS-IS and OSPF interior gateway protocol (IGP) protocols from 1 Tbps to 4 Tbps. The default bandwidth is 100 Mbps. You can increase the reference bandwidth to adjust the path metrics, which you use to determine the preferred path in case of multiple equal-cost routes to a destination.

  To configure the reference bandwidth, use the `reference-bandwidth` *reference-bandwidth* statement at the [`edit protocols isis`] hierarchy level or the [`edit protocols (ospf | ospf3)`] hierarchy level.

  [See reference-bandwidth (Protocols IS-IS) and reference-bandwidth (Protocols OSPF).]

- **Fast lookup of origin and neighbor ASs (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10004, PTX10008, PTX10016, QFX5130-32CD, QFX5700, and QFX5220)**—Starting in Junos OS Evolved Release 22.3R1, you can use the new `asregex-optimize` configuration statement at the [`edit policy-options defaults`] hierarchy level to perform a fast lookup of origin and neighbor autonomous systems (ASs). The `asregex-optimize` configuration statement is not enabled by default.

[See Improve the Performance of AS Path Lookup in BGP Policy.]

- **Synchronous Ethernet with G.8262 Standard Support (ACX7509)**—Starting in Junos OS Evolved Release 22.3R1, ACX7509 routers support Synchronous Ethernet features compliant with the following International Telecommunication Union Telecommunication Standardization (ITU-T) standards to facilitate the transference of clock signals over the Ethernet physical layer.

  - Synchronous Ethernet (G.8262) – Timing and synchronization aspects in packet networks. Specifies timing characteristics of synchronous Ethernet equipment clock (EEC).

  - Synchronous Ethernet Enhanced (G.8262.1)

Services Applications

- **Paragon Active Assurance test agent (ACX7100 and ACX7509)**—Starting in Junos OS Evolved Release 22.3R1, we support installing a test agent for Paragon Active Assurance Release 4.0.0. This remotely controlled, software-based active assurance solution gives you an easy way to test, monitor, and troubleshoot the data plane.

  [See Install the Paragon Active Assurance (PAA) Test Agent.]

- **IPv6 link-local address support for TWAMP Light (ACX7100, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—

  Starting in Junos OS Evolved Release 22.3R1, you can specify IPv6 link-local addresses for target addresses. To configure a Two-Way Active Measurement Protocol (TWAMP) Light target address as an IPv6 link-local address, include the `local-link` *logical-interface-name* option on the `target` statement at the [edit services monitoring twamp client control-connection *connection-name* test-session *session-name*] hierarchy level and include the `control-type light` statement at the [edit services monitoring twamp client control-connection *connection-name*] hierarchy level.

  [See Configure TWAMP on ACX, MX, M, T, and PTX Series Routers, EX4300 Series, EX9200 Series, and QFX10000 Series Switches.]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **SPRING support for SR-TE (ACX7024)**—Starting in Junos OS Evolved 22.3R1, we support the following features:

  - Segment routing policy to steer labeled or IP traffic at ingress routers

  - Segment routing paths for a non-colored static label-switched path (LSP)

  - Color-based traffic steering of Layer 2 and Layer 3 VPN services

  - SR policy-based dynamic tunnel module triggered SR-TE

  - Indirect next hop and composite next hop modes

[See Segment Routing Traffic Engineering at BGP Ingress Peer Overview.]

Software Installation and Upgrade

- **Hotfix support (ACX7024)**—Starting in Junos OS Evolved 22.3R1, support for hot fix using a delivery mechanism of full .iso images.

  [See request system software add and show system software list .]

- **Support for limited image version of Junos OS Evolved (ACX7024)**—Starting in Junos OS Evolved Release 22.3R1, the ACX Series devices ACX7024-DC-1PSU-L, ACX7024-DC-2PSU-L, ACX7024-AC-1PSU-L, ACX7024-AC-2PSU-L, and ACX7024-CHAS-L support the Junos OS Evolved limited image.

  The Junos OS Evolved limited image do not have cryptographic support and are intended for countries in the Eurasian Customs Union (EACU). These countries have import restrictions on software containing data-plane encryption.

  [See Junos OS Evolved Installation Packages.]

Additional Features

We have extended support for the following features to these platforms:

- **BGP PIC edge support for inet and MPLS VPNs** (ACX7024, ACX7100-32C, ACX7100-48L, and ACX7509)

  The following features are not supported:

  - Session-based repair

  - BGP PIC over LDP over RSVP tunnel

  - BGP PIC over SR-MPLS

  - BGP PIC with RSVP

  - BGP-LU with PIC

  - BGP PIC Edge protection for Layer 2 Services

  - Protection with multilink failure

  [See Configuring BGP PIC Edge for MPLS Layer 3 VPNs and Use Case for BGP PIC for Inet.]

- **Enhanced rapid ping command output (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016,QFX5130-32CD, QFX5220, and QFX5700)**— Output for ping commands using the rapid option now displays the following symbols:

- "!" for echo reply packets received within 500 ms

- "." for echo reply packets not seen within 500 ms

- "C" for received responses where the checksum of the reply is bad

[See ping.]

- **Layer 3 routing and protocols statistics for JTI (ACX7024)**

  [See Telemetry Sensor Explorer.]

- **Limited image version support of Junos OS Evolved** (ACX7509)

  This limited image does not have data-plane encryption and is intended only for the countries of the Eurasian Customs Union (EACU). These countries have import restrictions on software containing data-plane encryption.

  [See Junos OS Evolved Installation Packages.]

- **NSR (Nonstop active routing) support for NG-MVPN (next-generation multicast virtual private network) with multipoint LDP point-to-multipoint LSP as provider tunnel** (ACX7509)

  [See Multiprotocol BGP MVPNs Overview.]

- **OpenConfig LACP configuration support (ACX7100 and ACX7509)**

  [See Mapping OpenConfig LACP Commands to Junos Configuration.]

- **OpenConfig LACP and LLDP configuration support (ACX7100-32C, ACX-7100-48L, and ACX7509)**

  [See Mapping OpenConfig LACP Commands to Junos Configuration and Mapping OpenConfig LLDP Commands to Junos Configuration.]

- **OpenConfig LLDP configuration support (ACX7100 and ACX7509)**

  [See Mapping OpenConfig LLDP Commands to Junos Configuration.]

- **Operational command RPC support for returning JSON and XML output in minified format in NETCONF sessions (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016, QFX5130-32CD, and QFX5220)**

  [See Specifying the Output Format for Operational Information Requests in a NETCONF Session.]

- **RPM and TWAMP statistics sensor support for JTI (ACX7100-32C, ACX7100-48L, ACX7024, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**

  [See Telemetry Sensor Explorer.]

- **Packet Forwarding Engine timestamping for Two-Way Active Measurement Protocol (TWAMP) IPv6 test probes** (ACX7100, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)

  [See offload-type.]

- **Support for 802.1X authentication on Layer 2 and Layer 3 interfaces** (ACX7024,ACX7100-32C, ACX7100-48L, and ACX7509)

  [See 802.1X Authentication.]

- **Support for BGP flow specification** (ACX7100-32C, ACX7100-48L, and ACX7509)—BGP flow specification provides traffic filtering support based on the match conditions and actions. You can configure BGP flow specification (BGP flowspec) filters with "Redirect" action on ACX series routers.

  The following match conditions are not supported:

  - Fragment for IPv6

  - Packet length

  - Port

  - Source/destination prefix with offset

  The following actions are not supported:

  - Community

  - Next-term

  - Routing instance

  - Sample

  - Traffic marking

  [See Understanding BGP Flow Routes for Traffic Filtering.]

- **Support for control word and load-balancing capabilities using entropy and flow-aware transport of pseudowires (FAT) flow labels, across LDP-signaled pseudowires for virtual private LAN service (VPLS)** (ACX7024, ACX7100-32C, ACX7100-48L, and ACX7509)

  [See control-word, Configuring Entropy Labels, and FAT Flow Labels Overview.]

- **Support for EVPN-MPLS features** (ACX7024, ACX7100-32C, ACX7100-48L, and ACX7509)

  Support includes:

  - IRB with IPv4 and IPv6 addresses

- IRB virtual gateway

- IRB anycast gateway

- IRB with static mac

- EVPN asymmetric Type 2 and symmetric Type 5 routes

- EVPN E-LAN over BGP-LU

- EVPN proxy ARP and ARP suppression, and NDP and NDP suppression

- EVPN routing policies

- Ingress virtual machine traffic optimization (VMTO)

[See EVPN with IRB Solution Overview, Anycast Gateways, Symmetric Integrated Routing and Bridging with EVPN Type 2 Routes, Understanding EVPN Pure Type 5 Routes, EVPN Proxy ARP and ARP Suppression, and Proxy NDP and NDP Suppression, Ingress Virtual Machine Traffic Optimization, and Routing policies for EVPN.]

- **Support for interface-mode access, interface-mode trunk, and VLAN member configuration options** (ACX7509 and ACX7024))

  [See Bridging and VLANs.]

- **Support for Multi-Chassis Link Aggregation Groups (MC-LAGs) (ACX7509)**—Starting in Junos OS Evolved Release 22.3R1, the following features are available on MC-LAGs:

  - Layer 2 bridging for active-active and active-standby modes

  - Layer 2 and Layer 3 multicast with and without IGMP or MLD snooping

  [See Understanding Multichassis Link Aggregation Groups.]

- **Support for the NTP restrict command** (ACX7509, PTX10004, PTX10016, and QFX5700)

  [See Configuring NTP Access Restrictions for a Specific Address (SRC CLI).]

- **Support for unnumbered interfaces** (ACX7024, ACX7100-32C, ACX7100-48L, and ACX7509)

  Support includes:

  - Bidirectional Forwarding Detection (BFD)

  - Border Gateway Protocol (BGP)

  - BGP labeled unicast

  - Ethernet VPN virtual private wire service (EVPN-VPWS)

- IS-IS protocol adjacency

- Label Distribution Protocol (LDP)

- Layer 2 VPN/Layer 2 circuit

- Layer 3 VPN

- Qualified next hop

- Resource Reservation Protocol - Traffic Engineering (RSVP-TE)

- Static Subnet route

- Source Packet Routing in Networking (SPRING) over OSPFv2

- SPRING-TE

- Segment Routing (SR) with Multiprotocol Label Switching (MPLS)

- Static-LSP

[See Configure Unnumbered Interfaces.]

- **Support for SRv6 network programming in BGP and IS-IS** (ACX7024,ACX7100-32C, ACX7100-48L, and ACX7509)

[See Understanding SRv6 Network Programming and Layer 3 Services over SRv6 in BGP and How to Enable SRv6 Network Programming in IS-IS Networks.]

What's Changed

IN THIS SECTION

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

What's Changed in Release 22.3R1-S2

Junos XML API and Scripting

- The `file copy` command supports only text-formatted output in the CLI (ACX Series, PTX Series, and QFX Series)—The `file copy` command does not emit output when the operation is successful and supports only text-formatted output when an error occurs. The `file copy` command does not support using the `| display xml` filter or the `| display json` filter to display command output in XML or JSON format in any release. We've removed these options from the CLI.

What's Changed in Release 22.3R1

General Routing

- **CPU utilization greater than 100% (ACX Series)** —On ACX Series routers running Junos OS Evolved, the `show system processes` command might report CPU utilization spikes greater than 100%. This kind of CPU utilization is normal behavior, and no user action is required. The CPU utilization spikes represent the sum of individual processor threads and not of the entire system CPU capacity.

[See show system processes.]

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

- **Support for PKI daemon (ACX7024)**— We've introduced support for public key infrastructure (PKI) daemon on ACX7024 routers. The PKI daemon provides support to create two kinds of digital certificates on the device: a local certificate and a CA certificate. Using the local certificate, any remote resource can verify the device's identity. Using the CA certificate, the device can verify the identity of a remote resource by verifying the remote resource's digital certificate. A secure channel between the device and the remote resource is created only after this mutual verification. You can use the PKI configuration and operation commands to perform PKI operations on ACX7024 routers.

  [See Public Key Infrastructure (PKI).]

- **sFlow configuration**— sFlow configuration is allowed only on et, xe, and ge interfaces in EVO-based platforms. All other interfaces are blocked for configuring sFlow on EVO platforms. A cli error will be thrown if sFlow is configured on any other interface other than et, xe or ge interface.

- **Enhanced SSH hostkey algorithm configuration**—We've introduced the `hostkey-algorithm-list` statement at the [`edit system services ssh`] hierarchy level. This enhancement enables you to configure only the specified SSH hostkey algorithms. The system disables the remaining unspecified hostkey algorithms. In earlier releases, you need to disable the hostkey algorithms explicitly. All the hostkey algorithms at this hierarchy are enabled by default. The DSS algorithm is no longer available at this new hierarchy level.

  In addition, we've deprecated the `hostkey-algorithm` statement at the [`edit system services ssh`] hierarchy level.

  [See hostkey-algorithm.]

- **Instance type change is not permitted from default to L3VRF in open configuration (ACX Series and QFX Series)**—DEFAULT_INSTANCE is the primary instance that runs when there is no specific instance type configured in the route `set routing-options?`. Any instance you explicitly configure is translated into `set routing-instance r1 routing-options?`. The issue appears in translation, when you change instance type DEFAULT_INSTANCE (any instance to DEFAULT_INSTANCE) to L3VRF or L3VRF to DEFAULT_INSTANCE. As a result, such changes are not permitted. Additionally, DEFAULT_INSTANCE can only be named DEFAULT, and DEFAULT is reserved for DEFAULT_INSTANCE, therefore allowing no such changes.

- Prior to this change when route sharding is configured the output of CLI `show route` commands included information about sharding. After the change the use must add the **rib-sharding all** argument to CLI `show route` commands to display sharding information.

- **Support for configuring multi-chassis protection at the global level (ACX7509)**—We've enabled the multi-chassis-protection statement at the edit multi-chassis global hierarchy level for ACX7509 devices. In earlier releases, multi-chassis-protection could only be enabled at the interface level.

- The traffic rate could display incorrect values in the `show services inline ip-reassembly statistics fpc x pfe-slot y` output.

Juniper Extension Toolkit (JET)

- **Python 3 is the default and only Python version for executing Juniper Extension Toolkit Python scripts (ACX Series, PTX Series, and QFX Series)**—Junos OS Evolved supports only Python 3 for executing Juniper Extension Toolkit (JET) scripts written in Python. Python 2.7 is no longer supported for executing JET scripts, and we've deprecated the `language python` statement at the `[edit system scripts]` hierarchy level.

  [See Understanding Python Automation Scripts for Junos Devices.]

Junos XML API and Scripting

- **Deprecated functions in the `libpyvrf` Python module (ACX Series, PTX Series, and QFX Series)**—The `libpyvrf`Python module no longer supports the `get_task_vrf()` and `set_task_vrf()` functions.

  [See How to Specify the Routing Instance in Python 3 Applications on Devices Running Junos OS Evolved.]

- **Python 3 is the default and only Python version for executing commit, event, op, and SNMP Python scripts (ACX Series, PTX Series, and QFX Series)**—Junos OS Evolved supports only Python 3 for executing commit, event, op, and SNMP scripts written in Python. Python 2.7 is no longer supported for executing these types of scripts, and we've deprecated the `language python` statement at the `[edit system scripts]` hierarchy level.

  [See Understanding Python Automation Scripts for Junos Devices.]

MPLS

- Starting with Junos OS and Junos Evolved release 21.4R3, a CSPF LSP uses a new instance ID when attempting to re-signal a down LSP.

- **Display flexible algorithm information for SRv6 locators in TED database**—Use the `show ted database extensive` command to view the metric, flags, and flexible algorithm information associated with a SRv6 locator. Prior to this release, this information was not included in the TED database.

  [See show ted database.]

Network Management and Monitoring

- **Python 3 is the default and only Python version for executing YANG action and translation Python scripts (ACX Series, PTX Series, and QFX Series)**—Junos OS Evolved supports only Python 3 for executing YANG action and translation scripts written in Python. Python 2.7 is no longer supported for executing YANG action and translation scripts, and we've deprecated the `language python` statement at the `[edit system scripts]` hierarchy level.

  [See Understanding Python Automation Scripts for Junos Devices.]

- **Enhancement to the jnxRmonAlarmState (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series)**—You can now view the following additional values for the jnxRmonAlarmState when you use the show snmp mib walk jnxRmonAlarmTable: fallingThreshold (6) - If the value is less than or equal to falling-threshold risingThreshold (5) - If the value is greater than or equal to rising-threshold getFailure (7)- If the value is any value other than noError for the current internal 'get' request In earlier releases, you could view only the following status for the jnxRmonAlarmState: unknown (1), underCreation (2), or active (3).

Platform and Infrastructure

- **Enhanced bandwidth and burst policer value**—We've updated the default bandwidth value from 20000 to 100 pps and burst policer value from 20000 to 100 packets.

  [See show ddos-protection protocols parameters.]

- Starting Junos Evolved release 22.3R1, support is provided to limit Network Time Protocol (NTP) configuration to one address family (inet vs inet6). You can configure one source-address per inet and inet6 family for each routing-instance in NTP. For example, the following configuration is valid: `set system ntp source-address 2620:149:1d06:100::1 set system ntp source-address 10.10.10.100`.

System Management

- **Command to automate SSH key-based authentication (ACX Series, PTX Series, and QFX Series)**—You can set up SSH-key based authentication between the network device and a remote host by issuing the `request security ssh password-less-authentication` operational mode command. When you execute the command with the appropriate options, the device generates SSH keys for the current user, provided the user does not already have existing keys, and transfers the user's public key to the **authorized_keys** file of the specified user on the remote host.

  [See request security ssh password-less-authentication.]

Timing and Synchronization

- **Performance monitoring time interval with UTC on Junos OS Evolved platforms** —The performance monitoring (PM) time interval for 1-day bins on Junos OS Evolved platforms begins at midnight in the UTC zone, aligning with the standard behaviour of Junos OS. This synchronization allows you to maintain consistent performance monitoring schedules across platforms, enhancing the accuracy and reliability of network performance data.

User Interface and Configuration

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

  [See temperature-sensor.]

- **Persistent CLI timestamps**—To have a persistent CLI timestamp for the user currently logged in, enable the `set cli timestamp` operational command. This ensures the timestamp shows persistently for each new line of each SSH session for the user or class until the configuration is removed. To enable timestamp for a particular class with permissions and format for different users, configure the following statements:

```
set system login class class name permissions permissions
set system login class class name cli timestamp set system login user username class class
name authentication plain-text-password
```

> **NOTE**: The default timestamp format is %b %d %T. You can modify the format per your requirements. For example, you can configure the following statement:
>
> ```
> set system login class class name cli timestamp format "%T %b %d
> ```

  To enable timestamp for a particular user with default class permissions and format, configure the following statements:

```
set system login user username class class name authentication plain-text-password
set system login user username cli timestamp
```

Known Limitations

Learn about limitations in this release for ACX Series routers.

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

General Routing

- ACX7024:ACX7100-48L:: PTP to PTP noise transfer fails for the following frequencies:

  - 0.03125 HZ

  - 0.123125 HZ

  PR1608786

- syncE to PTP and syncE to 1pps noise transfer fails for the following frequencies on ACX7100-48L:

  - 0.00781 HZ

  - 0.00781 HZ

  - 0.01563 HZ

  - 0.03125 HZ

  - 0.06156 HZ

  - 0.12313 HZ

  PR1608866

- syncE to PTP and syncE to 1pps transient response marginally fails. This happens when the servo gets the initial 100ns jump in one measurement window and the next 100ns in the next measurement window adjusting less initially. PR1608934

- On ACX7100-48L or ACX7024, enabling or disabling of PTP TC or BC causes all interfaces to flap at the same time.PR1609927

- ACX7100-32C: PTP to PTP noise transfer fails for frequency 0.03125 HZ. PR1611838

- G.8275.1- G.8273.2 1PPS cTE performance might be outside class-C when using channelized 10G ports for PTP BC on ACX7100-32C. On each reboot, the 1PPS cTE measurement might be within the class-C measurement threshold, or might randomly be out of it by a few nanoseconds.PR1629819

- G.8275.1- G.8273.2 Packet cTE performance might be outside class-C when using channelized 25G ports with 100G ports for PTP BC on ACX7100-32C. On each reboot, the Packet cTE measurement might be within the class-C measurement threshold, or might randomly be out of it by a few nanoseconds.PR1637268

- SyncE and Hybrid PTP is not supported on the 1G interface on ACX7024. PR1644975

- ACX7024: syncE to PTP and syncE to 1pps noise transfer tests fails for the following frequencies:

  - 0.00781 HZ

  - 0.01563 HZ

  - 0.03125 HZ

  - 0.06156 HZ

  - 0.12313 HZ

  PR1649055

- The timingd restart is not supported on ACX7024. PR1651554

- G.8275.1.enh 2Way cTE performance might be outside class-C when using channelized 25G ports with 40G ports for PTP BC on ACX7100-32C. On each reboot, the 2Way cTE measurement might be within the class-C measurement threshold, or might randomly be out of it by a few nanoseconds.PR1662367

- The `request system snapshot` command is not supported on ACX7024. PR1686610

Routing Protocols

- When NSR is enabled on routers with non-forwarding routing-instance having BGP peers, the BGP peers in that instance are not successfully replicated to the backup RPD. PR1648707

Open Issues

Learn about open issues in this release for ACX Series routers.

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

EVPN

- On all Junos OS Evolved platforms that support EVPN-MPLS (Ethernet Virtual Private Networks - Multiprotocol Label Switching) services, during switchover or l2-learning restart, some EVPN next hops are not correctly associated with the routing instance in the Routing Engine impacting the traffic forwarding. PR1633344

- On performing graceful Routing Engine swithchover on ACX7509 platform with EVPN services, some physical interfaces are missing. The physical interfaces come up post reboot.PR1646722

- On ACX7024 ::Pseudo wire setup and tear down rate might be low. This is due to system CPU limitation.

General Routing

- On the ACX platform running Junos OS Evolved, you cannot clear or reset the disk option specified in the scheduled `request node reboot` command. The node reboots with the disk option last specified. PR1517596

- In some corner cases, traffic is not scheduled equally between strict priority queues. This can happen in the following scenario. Priority queue configured and completely utilizes the bandwidth and remaining queues are starved and traffic completely drops on those queues. In this state if we configure a second strict high priority queue, traffic is not scheduled equally between strict priority queues. This is a hardware specific issue, ACX7509 specific. If we have a shaper on priority queue this issue does not happen. Also if the traffic starts after the configurations no issues seen.PR1577035

- ACX7509: some of the interfaces from 16x100G and 20XSFP56 does not go down after evo-pfemand restart. PR1592388

- The timingd application cannot be successfully restarted on ACX7100 or ACX7024 with G.8275.1 profile configuration. If there are PTP streams configured and there is a timingd restart due to timingd core dump or requested application restart, the PTP streams might not be restored correctly, and changes to the PTP stream configuration after the restart might result in PTP streams that do not forward data packets correctly. It is very likely that a restart always affect the streams.PR1597120

- G.8275.1- G.8273.2 1PPS cTE performance might be marginally outside class-C for PTP BC on ACX7100-48L, especially for mixed speed port testing with combinations of 10G / 25G channelized ports and 100G ports. On each reboot, the 1PPS cTE measurement might be within the class-C measurement threshold, or might randomly be out of threshold by a few nanoseconds.PR1607381

- A restart of DHCP takes more time because of internal issues with the SIGTERM event. PR1610229

- In ACX7509, 1GE interface does not come up with copper 1G SFP-T optics and this issue is specific to copper 1G cables. PR1614286

- On ACX Series platforms, 400G DAC flap might be seen after OIR, FPC restart, device reboot enabling or disabling interface.PR1618488

- On ACX Series devices, ungraceful removal (OIR) of FPC or an FPC fault might result in a PCIE MAJOR alarm **PCI Uncorrected error on dev 0000:00:03.0** which does not get cleared. The only way to clear this alarm is reboot of the device. There are 2 situations in which this alarm can be seen:

  1. **FPC is faulty**: In rare FPC fault cases, the PCI Uncorrected error alarm might be seen along with FPC going to a Fault state as indicated by the `show chassis fpc` command. This is accompanied by other FPC major alarms. Once the faulty FPC is replaced with a good one, the alarm is still seen, and a reboot is required to clear this alarm. Post identification of the fault and FPC replacement, this alarm is harmless, and FPC state can be confirmed through the `show chassis fpc` command.

  2. **Ungraceful OIR**: The ungraceful removal of FPCs is not recommended. This operation might result in PCI Uncorrected Error alarm.

  Use one of the following two methods to do a graceful FPC OIR removal:

  - Execute the `request chassis fpc slot <slot > offline` command from the CLI.

- Press the Offline Button for 1 second on the FPC to offline the FPC. Once the FPC is gracefully offlined both LEDs - PWR and STS go off. The FPC can be removed at this point.

  PR1620197

- If a system is fully scaled across features and firewall is also scaled, CPU consumption might be more for a small window of around 5 seconds after every 18 seconds or so. Evo-pfemand might be busy collecting the scaled firewall statistics for that 5 second window and any other applications such as **pfe-cli** trying to execute commands might fail during it. PR1629342

- When CLI based trigger of FPC restart is given and subsequently a Routing Engine switchover event is triggerred, before the FPC's have come back online - the FPC's might not come online after switchover. It can be stuck in offlining or Fault state.PR1645305

- On ACX7509 platforms, interface flaps are seen on performing primary role switchover using the primary Routing Engine offline button press. Traffic drop is seen due to interface flap. PR1668509

- ACX7024: With high scale of L3VPN VRF instances system CPU usage might continue to be high. PR1655310

- After channelizing 100G port to 4x25G on ACX7024, channelized ports do not come up if FEC is set to FEC74. PR1684770

Routing Protocols

- ACX7024: The rpd process might generate core file seen after removal or restoration of configuration. This occurs rarely. PR1683239

Services Applications

- When the Paragon Active Assurance (PAA) Test Agent path trace measurement is running on the ACX7100 and ACX7509 routers, you might randomly see the error event **Hardware timestamp error** when the combined bandwidth of all of the running tests exceeds 140 Mbps. PR1674211

- A Paragon Active Assurance (PAA) Test Agent running on ACX7100 and ACX7509 might report significant jitter spikes, sometimes exceeding 40ms in latency measurements, even in an idle system. These spikes might originate from the device and do not necessarily represent actual network latency. The data plane forwarding performance is not affected by this issue. PR1680309

- When the Paragon Active Assurance (PAA) Test agent is running a UDP test at a rate exceeding 140 Mbps, packet drops might occur. Packet drops are caused by a too small receive buffer. Increase the receive buffer in the PAA UDP test settings to 1000000 to resolve the issue. PR1686327

User Interface and Configuration

- The system might ask for your password when you are trying to save configuration file. PR1665008

Resolved Issues

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

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

Class of Service (CoS)

- Junos OS Evolved:ACX: When fixed classifier is detached all default classifiers must be re-attached.PR1649163

EVPN

- VxLAN encapsulation might fail to forward traffic to remote devices. PR1639204

- EVPN VXLAN Type 5 does not work with asymmetric VNI configuration. PR1652339

General Routing

- ACX7509 :: picd core file is observed when we restart FPC with 700k scaled MAC. PR1602352

- [interface] [ACX7509] Interfaces mapped to same BCM port group flap when any one of the interfaces speed is modified.PR1608223

- [ECMP] ACX7509 : ::Picd core (0x00007f3d44b115da) file is observed when we restart FPC with 32000 ECMP groups scale. PR1609389

- PTP performance might randomly become bad for 30 minutes. PR1614309

- On ACX7509, details of auto negotiation settings are not available on 1GigE interfaces. PR1621991

- ACX7509 **PCI Device missing FPC[0] FPC Supercon FPGA** alarm reported on all FPCs. PR1627348

- After picd or rpdagent app restart multiple object-info anomalies for evo-pfemand are seen. PR1628843

- Traffic loss is seen after the VRRP primary role switch. PR1633986

- [Platform] : ACX7509: Observing hwdre core file at HwdAppStopObserver after upgrade to 21.4R1.13. PR1636243

- In ACX7509, on multiple FPC restarts, link does not come up with huge FEC errors. PR1639666

- The rpd-agent process might crash with a high scale of member nexthops. PR1640224

- On ACX7100 or ACX7509 platforms, a few control packets get forwarded on ERPS discarding port also, leading to traffic loop. PR1641454

- Junos OS Evolved infrastructure check fails with memory leak, evo-pfemand error. PR1641947

- The `show system core-dumps routing-engine both` command does not display anything on ACX7509. PR1646266

- Non-standard optics causes pcid core file issue. PR1649925

- TCAM field group entry shuffle is not traffic safe. PR1650266

- ACX7509 :: picd/evo-pfemand core is observed occasionally when we perform restart FPCs with multi-D system scale. PR1650302

- The classification-override functionality does not work for IPv6 traffic. PR1650622

- On ACX7100 or ACX7509 OAM link fault management (LFM) discovery state is not correct. Discovery state is either `Active Send Local` or `Fault`. PR1651580

- Approximately 15-20 seconds of IPv6 traffic loss after GRES. PR1655374

- [timing] [ptp] G.8275.2.enh- T-BC stuck in `acquiring` state with bad CF values in channelized ports. PR1657531

- On ACX7509, clockd core file and interfaces going down might be observed after repeated switchover operations. PR1657981

- The jdhcpd process might be stuck at 99% if `traceoptions` is enabled in high DHCP traffic scenarios. PR1658087

- ACX7100-32C:ACX7100-48L::jdhcpd core file seen on boot. PR1658327

- The object-info anomalies reported for picd relating to pfeE while testing switchover. PR1662411

- The hwdre and evo-pfemand applications might crash if idmd, fabtoken and hwdre are restarted immediately after an FEB offline. PR1669130

- Switchover caused by master RCB power-fault might cause links to go down. PR1669162

- Rare traffic stall in scaled scenarios on FEB offline or online. PR1669211

- The `show system alarm` CLI command shows **Optics does not support configured speed** minor alarm for few 1G optics. PR1671200

- ACX7509 HA: Backup FEB1 links down after primary FEB0 restart. PR1673274

Interfaces and Chassis

- On ACX7509 devices, there is a limitation in adding more than 64 member links in 1 LAG, whereas from ASIC, there is no limitation. PR1627951

Platform and Infrastructure

- The line cards MPC10 or MPC11 or LC-9600 might crash on Junos OS Evolved platforms.
  PR1667716

User Interface and Configuration

- The traffic might not flow after deleting or adding VLAN configuration with `load override`. PR1647853

Junos OS Evolved Release Notes for PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016 Devices

IN THIS SECTION

- What's New | **48**
- What's Changed | **60**
- Known Limitations | **64**
- Open Issues | **66**
- Resolved Issues | **70**

These release notes accompany Junos OS Evolved Release 22.3R1 for PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016 Packet Transport Routers. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

What's New

IN THIS SECTION

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

To view features supported on the PTX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Evolved Release 22.3R1, click the Group by Release link. You can collapse and expand the list as needed.

- PTX10001-36MR
- PTX10003
- PTX10004
- PTX10008
- PTX10016

The following sections highlight the key features in this release.

Authentication and Access Control

- 802.1X authentication support (EX4400 and EX4650) — Starting in Junos OS Release 22.3R1, 802.1X authentication is supported on LAG interfaces. 802.1X is an IEEE standard for port-based network access control that authenticates users attached to a LAN port. It blocks all traffic to and

from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the RADIUS authentication server.

- **LPM and AES-128 support for TCP keychain authentication (PTX10004, PTX10008, QFX5130-32CD, and QFX5700)**—Starting in Junos OS Evolved Release 22.3R1, we support the following features for the keychain authentication of TCP sessions:

  - Longest prefix match (LPM)

  - Advanced Encryption Standard-128 (AES-128) algorithm

  [See Authentication for Routing Protocols.]

EVPN

- **Support for BPDU protection for EVPN-VXLAN (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 22.3R1, we support bridge protocol data unit (BPDU) protection for EVPN-VXLAN.

  [See Understanding BPDU Protection for EVPN-VXLAN.]

- **Loop detection for EVPN-VXLAN fabrics (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)**—You can configure loop detection on the server-facing Layer 2 (L2) interfaces of leaf devices in EVPN-VXLAN fabrics. This feature can detect the following types of Ethernet loops:

  - A loop between two interfaces with different Ethernet segment identifiers (ESIs). This loop is typically caused by miswiring fabric components.

  - A loop between two interfaces with the same ESI. This loop is typically caused by miswiring a third-party device to the fabric.

  After you enable loop detection, the interfaces periodically send multicast protocol data units (PDUs). If a loop detection-enabled interface receives a PDU, a loop is detected and the interface is brought down. You must bring the interface back up manually or wait until a revert-interval timer expires.

  To configure loop detection, include the `interface` *interface-name* configuration statement at the `[edit protocols loop-detect enhanced]` hierarchy level. You can also configure the following attributes on that interface:

  - `vlan-id`—Configure a VLAN ID if the interface is configured in the enterprise style. (The operating system supports service provider and enterprise styles of configuration for switch interfaces. Service provider style requires more configuration but provides greater flexibility. Enterprise style is easier to configure but offers less functionality. In enterprise style, you place logical interfaces into Layer 2 mode by specifying `ethernet-switching` as the interface family. You can configure the `ethernet-switching` option only on unit 0. You cannot bind a VLAN ID to unit 0.)

- `action`—Specify the action that occurs if the interface receives a PDU.

- `transmit-interval`—Specify the interval between PDU transmissions.

- `revert-interval`—Specify the interval after which the interface is brought back up.

[See EVPN-VXLAN Lightweight Leaf to Server Loop Detection.]

High Availability

- **NSR support for next-generation MVPN (PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 22.3R1, we support nonstop active routing (NSR) for next-generation multicast virtual private networks (MVPN).

  [See Understanding Next-Generation MVPN Network Topology.]

Interfaces

- **Support for interfaces channelization on 400G-ZR-M (PTX10001-36MR)**—Starting in Junos OS Evolved Release 22.3R1, we support channelization of one 100GbE, three 100GbE, and four 100GbE interfaces along with the existing two 100GbE interfaces on 400G-ZR-M.

  [See Port Speed on PTX10001-36MR Router Overview.]

- **Support for hold-time option on aggregated Ethernet interfaces (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 22.3R1, we support the hold-time option with up and down milliseconds on aggregated Ethernet interfaces. You can specify the hold-time value to use a damp shorter interface transitions milliseconds.

  [See hold-time.]

- **Output filter for discard interface (PTX10003)**—Starting in Junos OS Evolved Release 22.3R1, you can configure `inet family protocol` on the discard interface. Use this configuration to apply an output filter to the interface. When you apply the output filter, the action specified by the filter executes before the traffic discards.

  [See Discard Interface Overview]

Junos Telemetry Interface

- **400G-ZR and ZR+ optics sensor support (PTX10003 and PTX10008)**—Starting in Junos Evolved OS Release 22.3R1, Junos telemetry interface (JTI) supports optical channel state and performance monitoring sensors. The sensors stream statistics using Juniper proprietary remote procedure calls (gRPC) and gRPC Network Management Interface (gNMI). We also support both INITIAL_SYNC and target-defined subscriptions for these sensors.

  [See Telemetry Sensor Explorer.]

- **BGP policy sensor upgrade (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Release 22.3R1, JTI supports data model **openconfig-bgp-policy.yang** version 6.0.2 (upgraded from version 4.0.1). New BGP policy sensors are supported.

  [See Telemetry Sensor Explorer.]

- **DDoS native sensor support (PTX10008 and PTX10016)**—Starting in Junos OS Evolved Release 22.3R1, Junos telemetry interface (JTI) supports native distributed denial of service (DDoS) sensors to monitor DDoS violations. When a violation occurs, DDoS telemetry data is streamed to monitoring stations.

  See Telemetry Sensor Explorer.]

- **Telemetry support for firewall resource utilization (PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016)**—Junos OS Evolved Release 22.3R1 introduces telemetry support for firewall resource utilization statistics using the OpenConfig sensor **/components/component/integrated-circuit/pipeline-counters**. The sensor displays the total supported filter entries and the used entries in terms of count and bytes.

  [See Firewall Resource Utilization.]

- **Initial sync enhancement for FIBstreaming (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Junos OS Evolved Release 22.3R1 introduces improved performance time for the initial sync of telemetry statistics. This enhancement applies to subscription requests for the top-level sensor path **/network-instances/network-instance/afts**. The initial sync feature gives the collector a complete view of the current state of every field on the device for that sensor path.

  [See Enabling "INITIAL_SYNC" Subscription Mode through gNMI.]

- **Sensor for LSP name of MPLS next hops (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 22.3R1, Junos telemetry interface (JTI) supports the sensor **/network-instances/network-instance/afts/next-hops/next-hop/state/lsp-name**.

  [See Telemetry Sensor Explorer.]

- **MPLS RSVP-TE sensor support (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos Evolved OS Release 22.3R1, Junos telemetry interface (JTI) supports the data model **openconfig-mpls-rsvp.yang** version 4.0.0. It also supports the new RSVP-Traffic Engineering (RSVP-TE) sensors.

  [See Telemetry Sensor Explorer.]

- **MPLS OpenConfig configuration and sensor support (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 22.3R1, Junos telemetry interface (JTI) supports these data models:

  - **openconfig-mpls.yang** version 3.2.2

- **opencfig-mpls-types.yang** version 3.2.1

- **opencofig-mpls-te.yang** version 3.2.2

- **opencofig-mpls-static.yang** version 3.2.2

The release supports these OpenConfig configurations:

- MPLS global

- MPLS named-explicit-path

- MPLS tunnels

The release supports these state groups:

- MPLS tunnels

- MPLS named-explicit-path

- MPLS static label-switched-path

- MPLS-TE interface attributes

- MPLS tunnel state counters (dependent on the Packet Forwarding Engine)

[See Telemetry Sensor Explorer and Mapping OpenConfig MPLS Commands to Junos Configuration.]

- **Packet Forwarding Engine sensors for device monitoring, discard counters, and forwarding table occupancy in JTI (PTX10003)**—Junos OS Evolved Release 22.3R1 supports streaming Packet Forwarding Engine statistics to an external collector. You can subscribe to sensors for device monitoring, discard counters, and forwarding table occupancy by using the following resource paths:

  - **/interfaces/**

  - **/junos/system/linecard/packet/usage/**

  - **/junos/system/linecard/npu/memory/**

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

- **Support for FTI sensors (PTX10003)**—Junos OS Evolved Release 22.3R1 introduces telemetry support for flexible tunnel interface (FTI) sensors. You can subscribe to collect FTI statistics by using either OpenConfig or native Junos resource paths.

  For OpenConfig sensor support, see Telemetry Sensor Explorer. For native Junos support, see Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).

- **Telemetry support for CoS page drop reporting (PTX10003)**—Starting in Junos OS Evolved Release 22.3R1, you can collect statistics on packet drops caused by page timeouts by subscribing to the

resource path **/junos/system/linecard/page-drops/page-drop/**. Page drop statistics include page drop counter, interface information, and queue details.

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

- **Telemetry support for DDoS sensors (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Junos OS Evolved Release 22.3R1 introduces telemetry support for distributed denial-of-service (DDoS) sensors. You can stream DDoS statistics from a device to a collector by including the resource path **/junos/system/linecard/ddos/** in a subscription.

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

- **VLAN sensor support (PTX10001-36MR, PTX10003, PTX10004, and PTX10008)**—Starting in Junos OS Evolved Release 22.3R1, Junos telemetry interface (JTI) supports the data model **openconfig-vlan.yang** version 3.2.1, including VLAN sensor support.

  [See Telemetry Sensor Explorer.]

Network Management and Monitoring

- **sFlow technology support for exporting extended IPv4 and IPv6 tunnel egress structure (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos Evolved OS Release 23.1R1, sFlow technology supports the export of the Extended Tunnel Egress Structure fields for traffic entering IPv4 or IPv6 GRE tunnels. These additional attributes will provide information about the GRE tunnel into which a packet entering the device will get encapsulated. The GRE tunnel could be IPv4 or IPv6. The feature is supported only when sFlow is enabled in the ingress direction wherein firewall-based GRE happens on IPv4 or IPv6 packets.

  Specifically, the below fields are reported as part of this extended structure:

  - Protocol reported as value 0x2f (GRE)

  - Source IP (IPv4 or IPv6 address of the tunnel source)

  - Destination IP (IPv4 or IPv6 address of the tunnel destination endpoint)

  The other fields such as length, source port, destination port, TCP flags, and priority will be reported as zero.

  The feature is supported for the following traffic scenarios when ingress sFlow sampling is enabled:

  - Incoming IPv4 traffic that undergoes IPv4 GRE

  - Incoming IPv6 traffic that undergoes IPv4 GRE

  - Incoming IPv4 traffic that undergoes IPv6 GRE

  - Incoming IPv6 traffic that undergoes IPv6 GRE

[See Examples: Configuring BGP Multipath.]

- **Fast lookup of origin and neighbor ASs (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10004, PTX10008, PTX10016, QFX5130-32CD, QFX5700, and QFX5220)**—Starting in Junos OS Evolved Release 22.3R1, you can use the new `asregex-optimize` configuration statement at the [edit policy-options defaults] hierarchy level to perform a fast lookup of origin and neighbor autonomous systems (ASs). The `asregex-optimize` configuration statement is not enabled by default.

  [See Improve the Performance of AS Path Lookup in BGP Policy.]

- **Origin validation communities conversion to keywords (PTX10001-36MR, PTX10008, PTX10016, QFX5130-32CD, and QFX5220)**—Starting in Junos OS Release Evolved 22.3R1, you can choose to accept or reject the origin validation extended communities received from an external BGP (EBGP) peer. The default behavior of Origin Validation State Extended Community (OVS EC) is changed to rejected if received from an EBGP peer. You can configure OVS EC to accept the community when needed. We also support the configuration of distinguished communities with keywords (valid, invalid, and unknown) at all the three layers of the BGP configuration hierarchy: global, group, and per-neighbor. If you enable the OVS EC at a hierarchy level, it's enabled for the lower levels as well. However, you can choose to disable it explicitly at a lower layer if required in any instance.

  To accept origin validation communities from an EBGP peer, use `origin-validation accept` at the [edit protocols bgp ebgp-community-cleanup], edit protocols bgp group <group-name> ebgp-community-cleanup], or [edit protocols bgp group <group-name> neighbor <address> ebgp-community-cleanup] hierarchy level.

  To reject origin validation communities from an EBGP peer, use `origin-validation reject` at the [edit protocols bgp ebgp-community-cleanup], edit protocols bgp group <group-name> ebgp-community-cleanup], or [edit protocols bgp group <group-name> neighbor <address> ebgp-community-cleanup] hierarchy level.

  [See BGP Origin Validation.]

- **BGP LU Prefix SID redistribution between IGP domains (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)**— Starting in Junos OS Release 22.3R1, we support BGP Labeled Unicast (BGP-LU) prefix-sid redistribution between IGP domains. We also support installing an mpls.0 stitch route to a BGP-LU next-hop instance.

  To set prefix segment attributes, use the `set prefix-segment` statement at the [edit policy-options policy-statement <policy-name> term <tern-name> from] hierarchy level.

  You can now enable prefix-sid redistribution between BGP and IS-IS via policy configuration without specifying the index under prefix-segment. To do this, use the `set prefix-segment redristribute` option at the [edit policy-options policy-statement <policy-name> term <term-name> then] hierarchy level.

  [See Link-State Distribution Using BGP.]

- **Strengthening ARP/NDP Control for IPv4/IPv6 Networks (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**— To protect routers from DoS attacks that exploit IPv6's large address space, administrators can now configure limits on ARP/NDP neighbor entries using new CLI

commands. These limits, applied globally and per interface, help prevent resource exhaustion by controlling the number of cached entries. The system issues warnings at 80% capacity and logs errors when it reaches maximum limits, ensuring network stability during potential attacks.

[See nd6-max-cache.]

Services Applications

- **IPv6 link-local address support for TWAMP Light (ACX7100, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—

  Starting in Junos OS Evolved Release 22.3R1, you can specify IPv6 link-local addresses for target addresses. To configure a Two-Way Active Measurement Protocol (TWAMP) Light target address as an IPv6 link-local address, include the `local-link` *logical-interface-name* option on the `target` statement at the `[edit services monitoring twamp client control-connection` *connection-name* `test-session` *session-name*] hierarchy level and include the `control-type light` statement at the `[edit services monitoring twamp client control-connection` *connection-name*] hierarchy level.

  [See Configure TWAMP on ACX, MX, M, T, and PTX Series Routers, EX4300 Series, EX9200 Series, and QFX10000 Series Switches.]

Software Installation and Upgrade

- **Support for error third-party attachments (TPAs) on errored objects during route installations (PTX10008 and PTX10016)**—In a distributed system, states can be produced anywhere and consumed anywhere, making it difficult for a producer (for example, a PFE) to determine whether the system is in the correct state for the consumer (for example, an rpdagent). Starting in Junos OS Evolved Release 22.3R1, during route installations the consumer can now notify the producing application when there are errors in processing the state update sent by the producer. The producer then attaches a TPA object on top of the errored object with details of the error and publishes it. The errors generated have standard error numbers.

  The forwarding information base (FIB) telemetry daemon (FIBtd) also receives error notifications. Use the Junos telemetry interface (JTI) and remote procedure calls (gRPC) services to stream or export ON_CHANGE FIB statistics to an outside SDN collector. Set the collector to subscribe to xpath **/state/system/anomalies/fib/** to get both the IPv4 and IPv6 error routes.

  Use the CLI to query errored objects and related information. The consumer is notified when the errors are cleared and the route installation is successful.

  [See Error TPAs for Route Installation.]

Additional Features

We have extended support for the following features to these platforms:

- **Automatic LSP policing support on point-to-point LSPs** (PTX10001-36MR, PTX10004, PTX10008, PTX10016)

  [See Configuring Automatic Policers.]

- **Basic MVPN support with BGP sharding** (PTX10001-36MR, PTX10003, PTX10004, and PTX10008)

  [See Understanding BGP RIB sharding and BGP Update IO thread.]

- **CFM support (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)**

  - Up maintenance association end points (MEPs) in distributed periodic packet management (PPM)

  - Distributed Y.1731 on synthetic loss measurement (SLM), delay measurement (DM), and loss measurement (LM)

  - Down MEPs on bridges, circuit cross-connect (CCC) , and Ethernet VPN (EVPN)

  - Distributed session support for connectivity fault management (CFM) on aggregated Ethernet

  - Enhanced CFM mode

  - Inet support for Data Model (DM) and synthetic loss message (SLM)

  - Action profile for marking a link down, except for EVPN and bridge up MEP

  - LM colorless mode

  - DM and LM on aggregated Ethernet if all active child links are on the same Packet Forwarding Engine

  - Supported CFM protocol data units (PDUs), as follows:

    - Continuity check messages (CCM)

    - LBM

    - LBR

    - Link Trace Message (LTM)

    - Link Trace Reply (LTR)

    - 1DM

    - Delay measurement message (DMM)

    - Delay measurement reply (DMR)

    - LMM

- LMR

  - Synthetic loss message (SLM)

  - Synthetic loss reply (SLR)

- Enterprise and service provider configurations

- VLAN normalization

- VLAN transparency for CFM PDUs

- CoS forwarding class (FC) and CoS packet loss priority (PLP) for CFM

- CFM session on child physical interface in distributed mode

- SNMP

- Chassis ID or Send ID type, length, and value

- Trunk mode

- Maintenance association intermediate point (MIP)

[See Connectivity Fault Management (CFM).]

- **Enhanced rapid ping command output (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016,QFX5130-32CD, QFX5220, and QFX5700)**— Output for ping commands using the rapid option now displays the following symbols:

  - "!" for echo reply packets received within 500 ms

  - "." for echo reply packets not seen within 500 ms

  - "C" for received responses where the checksum of the reply is bad

  [See ping.]

- **Ethernet interface sensor support for Junos telemetry interface (JTI) (PTX10003)**

  [See Telemetry Sensor Explorer.]

- **Firewall filter match conditions support: next-header and payload-protocol** (PTX10003, PTX10001-36MR, PTX10004, PTX10008, and PTX10016)

  [See Firewall Filter Match Conditions for IPv6 Traffic.]

- **Firewall filter support** (PTX10016)

  [See Firewall Filter Match Conditions and Actions (PTX Series Routers).]

- **IGMP, MLD snooping support** (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)

  - In bridge domains

  - In integrated routing and bridging (IRB) enabled bridge domains

  [See IGMP Snooping Overview and Understanding MLD Snooping.]

- **Loose mode discard** (PTX10003)

  [See Configuring Unicast RPF Loose Mode with Ability to Discard Packets.]

- **MACsec bounded delay protection (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**

  [See Configuring Advanced MACsec Features.]

- **OISM in an EVPN-VXLAN fabric (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)**

  Support includes:

  - Optimized intersubnet multicast (OISM) server leaf, border leaf, and lean spine device roles

  - IGMPv2 or IGMPv3, IGMP snooping, and selective multicast Ethernet tag (SMET) route optimization

  - `vlan-based` and `vlan-aware` MAC-VRF EVPN instance service types

  - External multicast:

    - Multicast VLAN (M-VLAN) method

    - Classic L3 interface method

    - Non-EVPN IRB method

  [See Optimized Intersubnet Multicast in EVPN Networks.]

- **OpenConfig QoS configuration support (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**

  [See Mapping OpenConfig QoS Commands to Junos Configuration and Telemetry Sensor Explorer.]

- **Operational command RPC support for returning JSON and XML output in minified format in NETCONF sessions (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016, QFX5130-32CD, and QFX5220)**

  [See Specifying the Output Format for Operational Information Requests in a NETCONF Session.]

- **RPM and TWAMP statistics sensor support for JTI (ACX7100-32C, ACX7100-48L, ACX7024, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**

  [See Telemetry Sensor Explorer.]

- **Packet Forwarding Engine timestamping for Two-Way Active Measurement Protocol (TWAMP) IPv6 test probes** (ACX7100, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)

  [See offload-type.]

- **Support for CBF fallback inside service group** (PTX10008)

  [See source-routing-path.]

- **Support for class-of-service-based forwarding (CBF) support for colored static segment routing– traffic engineering (SR-TE)** (PTX10008 and PTX10016)

  [See source-routing-path.]

- **Support for disable, restart, offline, or online of individual Packet Forwarding Engine instances** (PTX10001-36MR)

  [See request chassis fpc and show chassis fpc.]

- **Support for the NTP restrict command** (ACX7509, PTX10004, PTX10016, and QFX5700)

  [See Configuring NTP Access Restrictions for a Specific Address (SRC CLI).]

- **Support for tunnel decapsulation using firewall filters for GRE and UDP tunnels** (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)

  [See Configuring a Filter to De-Encapsulate GRE Traffic and decapsulate (Firewall Filter).]

- **Uniform load balancing of point-to-multipoint (P2MP) traffic over aggregated links** (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)

  [See Point-to-Multipoint LSPs Overview.]

What's Changed

IN THIS SECTION

Learn about what changed in these releases for PTX Series routers.

What's Changed in Release 22.3R1-S2

Junos XML API and Scripting

- The `file copy` command supports only text-formatted output in the CLI (ACX Series, PTX Series, and QFX Series)—The `file copy` command does not emit output when the operation is successful and supports only text-formatted output when an error occurs. The `file copy` command does not support using the `| display xml` filter or the `| display json` filter to display command output in XML or JSON format in any release. We've removed these options from the CLI.

What's Changed in Release 22.3R1

Authentication and Access Control

- **Enhanced SSH hostkey algorithm configuration**—We've introduced the `hostkey-algorithm-list` statement at the [`edit system services ssh`] hierarchy level. This enhancement enables you to configure only the specified SSH hostkey algorithms. The system disables the remaining unspecified hostkey algorithms. In earlier releases, you need to disable the hostkey algorithms explicitly. All the hostkey algorithms at this hierarchy enabled by default. The DSS algorithm is no longer available at this new hierarchy.

  In addition, we've deprecated the `hostkey-algorithm` statement at the [`edit system services ssh`] hierarchy level.

  [See hostkey-algorithm.]

Class of Service (CoS)

- For PTX Series devices running Junos OS Evolved, software priority "medium-low" maps to hardware priority "medium" for normal scheduling mode and "low" for strict priority scheduling mode.

General Routing

- **Change in the `help syslog PFE` command output**—In Junos OS Evolved, the output for help syslog PFE command is fixed to be consistent with Junos OS output on PTX10008 device. ERRMSG tags in EVO are named as SFLOWD_ whereas in Junos they are named as PFE_SFLOW_.

- sFlow configuration? sFlow configuration is allowed only on et, xe, and ge interfaces in EVO-based platforms. All other interfaces are blocked for configuring sFlow on EVO platforms. A cli error will be thrown if sFlow is configured on any other interface other than et, xe or ge interface.

- **JNP10K-PWR-DC2 power supplies installed in PTX10008 and PTX10016 routers display as online when the power supplies are switched off**— JNP10K-PWR-DC2 power supplies installed in PTX10008 and PTX10016 routers in which Junos OS Release 21.4R1 or Junos OS Evolved Release 21.4R1 is installed display as online in the output of the command `show chassis environment psm` when the input power feeds are connected, but the power switch on the power supplies are switched off.

- Prior to this change when route sharding is configured the output of CLI `show route` commands included information about sharding. After the change the use must add the **rib-sharding all** argument to CLI `show route` commands to display sharding information.

- The traffic rate could display incorrect values in the `show services inline ip-reassembly statistics fpc x pfe-slot y` output.

Juniper Extension Toolkit (JET)

- **Python 3 is the default and only Python version for executing Juniper Extension Toolkit Python scripts (ACX Series, PTX Series, and QFX Series)**—Junos OS Evolved supports only Python 3 for executing Juniper Extension Toolkit (JET) scripts written in Python. Python 2.7 is no longer supported for executing JET scripts, and we've deprecated the `language python` statement at the `[edit system scripts]` hierarchy level.

  [See Understanding Python Automation Scripts for Junos Devices.]

Junos XML API and Scripting

- **Deprecated functions in the `libpyvrf` Python module (ACX Series, PTX Series, and QFX Series)**—The `libpyvrf`Python module no longer supports the `get_task_vrf()` and `set_task_vrf()` functions.

  [See How to Specify the Routing Instance in Python 3 Applications on Devices Running Junos OS Evolved.]

- **Python 3 is the default and only Python version for executing commit, event, op, and SNMP Python scripts (ACX Series, PTX Series, and QFX Series)**—Junos OS Evolved supports only Python 3 for executing commit, event, op, and SNMP scripts written in Python. Python 2.7 is no longer supported for executing these types of scripts, and we've deprecated the `language python` statement at the `[edit system scripts]` hierarchy level.

  [See Understanding Python Automation Scripts for Junos Devices.]

MPLS

- Starting with Junos OS and Junos Evolved release 21.4R3 a CSPF LSP uses a new instance ID when attempting to re-signal a down LSP.

Network Management and Monitoring

- **Python 3 is the default and only Python version for executing YANG action and translation Python scripts (ACX Series, PTX Series, and QFX Series)**—Junos OS Evolved supports only Python 3 for executing YANG action and translation scripts written in Python. Python 2.7 is no longer supported for executing YANG action and translation scripts, and we've deprecated the `language python` statement at the `[edit system scripts]` hierarchy level.

  [See Understanding Python Automation Scripts for Junos Devices.]

OpenConfig

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

Platform and Infrastructure

- Starting Junos Evolved release 22.3R1, support is provided to limit Network Time Protocol (NTP) configuration to one address family (inet vs inet6). You can configure one source-address per inet and inet6 family for each routing-instance in NTP. For example, the following configuration is valid: set system ntp source-address 2620:149:1d06:100::1 set system ntp source-address 10.10.10.100

- **Enhanced bandwidth and burst policer value**—We've updated the default bandwidth value from 20000 to 100 pps and burst policer value from 20000 to 100 packets. This enhancement avoids the CPU usage of `eventd` and `snmpd` reaching more than 100%. Earlier to this release, when the system receives a violated traffic for SNMP along with other protocols traffic, the CPU usage of `eventd` and `snmpd` was reaching more than 100% with an error.

  [See show ddos-protection protocols parameters.]

System Management

- **Command to automate SSH key-based authentication (ACX Series, PTX Series, and QFX Series)**—You can set up SSH-key based authentication between the network device and a remote host by issuing the `request security ssh password-less-authentication` operational mode command. When you execute the command with the appropriate options, the device generates SSH keys for the current user, provided the user does not already have existing keys, and transfers the user's public key to the **authorized_keys** file of the specified user on the remote host.

  [See request security ssh password-less-authentication.]

Known Limitations

IN THIS SECTION

Learn about limitations in this release for PTX Series routers.

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

General Routing

- If multiple sibs goes in to the `Offlining` state and halt the primary Routing Engine, the SIBs gets stuck in the `Offlining` state for sometime. Eventually the SIBs goes in to the `Offline` state. The `show chassis sibs` command must be used to check the state of the SIBs. PR1584712

- On all PTX platforms, addition or deletion of the filter configuration in loopback interface might result in error messages with some packet drop for short duration, which would be self-recovered. PR1589296

- IPv6 primary-only IP address does not move to the new primary Routing Engine after a switchover. As a workaround, you must deactivate and activate the primary-only IPv6 address on the primary Routing Engine. PR1648371

- When a fully loaded Scapa16 setup with line rate traffic reboots, sometimes few interfaces might experience traffic loss (reduced throughput). PR1649979

- Output filter cannot match the actual TTL value of packet for filter decapsulation traffic with no decrement ttl configured. PR1666673

Routing Policy and Firewall Filters

- IPv4 unsupported filter match `fragment-flags reserved` command should not be used, as the matches do not fragment traffic pattern as well. PR1676517

User Interface and Configuration

- In a dual-Routing Engine, assume ZTP process gets started on the primary Routing Engine node RE0. While ZTP and configuration commits on the primary Routing Engine RE0 (as part of ZTP) and configuration commit does not get completed on RE0. During this situation, if the Routing Engine switchover gets triggered then the configuration commit gets aborted or stopped ungracefully on the node RE0. The ZTP process gets started freshly on the new primary node Routing Engine RE1. Due

to the ungraceful exit of commit process on RE0, the ZTP might not succeed on the Routing Engine
RE1 because it might face commit failures on primary node Routing Engine RE1. PR1649786

Open Issues

Learn about open issues in this release for PTX Series routers.

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

General Routing

- Issue occurs only when the routing daemon crashes but does not impact on rest of the NSR support.
  PR1561059

- On PTX10001-36MR, the software driver reads the voltage threshold erroneously causing the `Host 0
  Voltage Threshold Crossed` alarm to present on the device. PR1592258

- Traffic loss observed on BGP-LU paths after restoring primary paths in setup with IGP/LDP RLFA
  enabled. PR1619229

- 400G ZR-M 740-131169 modules does not come up in the odd ports due to crossing temperature
  threshold, which results into optics shutdown. Manually configuring fan speeds to 100 percent does
  help in bringing the optics up. PR1631279

- System reboot or boot up with traffic might result in init time fabric link crc errors and cause traffic drop. PR1635178

- The 400G-ZR/400G-ZR-M optic transceiver firmware upgrade failures. It is a generic issue faced across all single RU platforms supporting QDD-400G-ZR/QDD-400G-ZR-M. PR1638284

- The next-header match in IPv6 firewall filter does not work as expected. The next-header matches the payload-protocol (last-header). PR1645401

- Sflow cannot populate extended router header or true OIF for packet traversing through ECMP in TEVRF or recovery VRF. PR1652202

- Junos OS Evolved does not support the following RPC:

```
// KillProcess kills an OS process and optionally restarts it.
 rpc KillProcess(KillProcessRequest) returns (KillProcessResponse) {}
```

PR1655652

- Junos OS Evolved does not support the mpls-any and mpls-inet-both-non-vpn multiple rewrite rules aggregated Ethernet on PTX devices running BT ASIC. The order of applying the rewrite rules is not correct. The non-VPN rewrite rule gets effect for the VPN traffic. PR1655653

- On adding filter to loopback interface, at times incorrect count gets displayed for the firewall policer. You must clear all firewall. PR1664600

- Junos OS Evolved does not support the GNOI API SetPackage through Remote Download. PR1665185

- Sometimes BGP and RSVP sessions remain down after quick arpd process disable and enable. Whenever you encounter such scenario, system can be recovered from erroneous state by executing `restart routing` gracefully in CLI. PR1665362

- On restarting the msvscd application, data does not get exported through the UDP query. PR1670826

- Junos OS Evolved supports mfg-name only for optics where those FRUs can be from different manufacturers. All other FRUs manufactured by Juniper do not stream mfg-name. PR1672697

- Fragmented packets have an additional next hop (frag) that causes the FLT to not match on ICMPv6 headers for lo0 filters. You must change the loopback MTU size. PR1675820

- Log clean-up process does not cover the Zookeeper log on PTX Series device running Junos OS Evolved and it could potentially cause impact to the system when the log file size occupies too much disk size. Manually cleaning up the log is required. PR1678880

- For PTX10001-36MR, `show system applications error` command is not available. PR1682045

- On Junos OS Evolved PTX Series device, application ZTP fails on node Re0 about one day later post system zeroize. PR1683964

Infrastructure

- The GRES triggered through the `request chassis routing-engine master switch` generates the following connector driver overlay messages: `{master} root@bowmore-05-re0> [ 1185.081257] gpio-jnx-i2cs gpio-jnx-i2cs.50: Asserting power_status irq 59 [ 1185.125182] OF: overlay: overlay_is_topmost: #9 clashes #10 @/ftc0/i2c-bus/i2cs@54/fan_hwmon [ 1185.125183] OF: overlay: overlay #9 is not topmost` PR1539232

- On all Junos Evolved OS platforms, the device might panic with vmcore under high memory pressure situations when kernel memory allocation fails. PR1646610

Interfaces and Chassis

- You must perform joji over the interface using `test picd optics fpc_slot <fpc slot> pic_slot <pic slot> port <port num> cmd oir_enable test picd optics fpc_slot <fpc slot> pic_slot <pic slot> port <port num> cmd remove test picd optics fpc_slot <fpc slot> pic_slot <pic slot> port <port num> cmd insert test picd optics fpc_slot <fpc slot> pic_slot <pic slot> port <port num> cmd oir_disable` command. PR1646915

MPLS

- Traceroute in MPLS OAM on SR over IPv6 might fail in ECMP incase PTX box is in topology. This occurs because of Linux kernel in the Junos OS Evolved puts an autoflowlabel on every IPv6 packet. This flow label is transparent to daemon process, which uses a null value for it and calculates the next hop details. Packet Forwarding Engine however takes the flow label into account and calculates the next hop details. This difference in calculation of next hop details leads to a mismatch in the path the packet takes to the destination and can cause traceroute to fail. PR1618406

- When the bypass host route was deprecated, bypass label information does not correctly set when you send the backup PathTear messages if long refresh interval gets disabled between the Point of Local Repair (PLR) and the Merge Point (MP). PR1685182

Network Management and Monitoring

- When you configure the `maximum-password-length` command and tries to configure password whose length exceeds the configured maximum-password-length, error messgae gets generated along with `error '(ok/)' tag` gets emitted. Ideally `'ok/>' tag` should not be emitted in an error scenario and the configuration does not get committed. PR1585855

- The mgd process crashes when you configure an invalid value for the identityref type leafs/leaf-lists while you configure openconfig or any other third-party YANG. Issue occurs with JSON and XML loads. PR1615773

Routing Policy and Firewall Filters

- On Junos OS Evolved platforms, the unsupported configuration of BGP flow spec `interface-group exclude` might lead to some errors and the Packet Forwarding Engine corruption, which does not permit filter bind. PR1639391

Routing Protocols

- When l2cpd (in the context of xSTP) clears the entries that it has programmed on ppmd, that is, when you delete xSTP configurations from the device, there can be a possibility of ppmd core file generation. If ppmd is in distributed mode then there is no service impact, else there can be service impact as packet transmission for various protocols happens if ppmd is in centralized mode. PR1660299

User Interface and Configuration

- When you terminate the evo-cda-bt process, fpc gets restarted. We might see agentd crash due to ungraceful FPC restarts. This issue is not seen in a normal working scenario and is seen only upon ungraceful fpc restarts. PR1655441

- The system might ask for your password when you are trying to save configuration file. PR1665008

Resolved Issues

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

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

Class of Service (CoS)

- The `show Class-of-service Interface` command might not display the classifier bind info on a physical interface with only Inet/Inet6 (without family mpls or not with any rewrite rules). PR1652342

General Routing

- On PTX10003 devices, in a scaled Layer 2 network, error logs gets printed for MAC creation. MAC-learning works as expected. PR1491933

- The `/interfaces/interface/subinterfaces/subinterface/state/counters` does not get exported during initial synchronization for on-change. PR1620160

- The cosd process might generate core file after the Routing Engine switchovers. PR1620758

- Junos OS Evolved does not supoort the GNOI RPC TransferToRemote. PR1625212

- Config-Sync failure alarm gets generated. PR1629952

- The aggregated Ethernet interface lacp member link gets stuck in the `Detached` status. PR1633849

- Traffic loss occurs after the VRRP mastership switches. PR1633986

- Auto RP base verification fails with multiple RPs with the same group range. PR1634982

- Label stack might be corrupted after the Packet Forwarding Engine restarts. PR1635130

- NPU util sensor to include FLT consumption for ZX and BT based PTX devices. PR1638487

- KRT queue entries get stuck during the Routing Engine switchover when the backup RPD is not yet ready. PR1641297

- The interfaces might remain down and loopback wedge error might occur. PR1645431

- The Routing Engine mastership might not transfer on each rpd crash. PR1645611

- Changing error severity does not work on FRUs managed by the Routing Engines. PR1647282

- `mac-vrf` does not support MAC limit configuration. PR1647327

- High inter-packet delay and throughput performance degrades the Packet Forwarding Engine sensors. PR1648133

- The rpd-agent process might restart post mastership switchover. PR1669767

- Modifying next hop that as indirect next hop address to set decapsulate_header does not work. PR1648162

- Firewall counters might not get incremented for a longer time. PR1649324

- On PTX10008 devices, SyncE clock `hold-off-time` configuration does not work due to incorrectly computed timer value. PR1649358

- The debug-collector does not collect the backup Routing Engine logs when SSH root-login configuration gets set to `deny`. PR1649647

- Sensors under `/components/component/integrated-circuit/backplane-facing-capacity/state/` do not exported in UDP through WAN port but exports in UDP through management port. PR1649876

- The `ZERO Queue Packets received on Queue: 1 Forwarding classes` message gets generated when you issue the `show interfaces queue egress ae1` command while checking queue 1 for IPv6 traffic. PR1650622

- Junos OS Evolved does not support HTTP or HTTPs as the tranfer for gnoi-based remote file transfer. PR1650828

- You must allow container to come up even if it has no CSPP interfaces. PR1651204

- The BFD session might flap in some scaled system with churn. PR1651473

- ECN bits on PTX platforms never gets set. PR1651830

- An error might get generated when you delete the member link on an aggregated Ethernet interface. PR1651932

- After configuring `rpf-check` on lag interface, the lag interface goes down. PR1652623

- P2MP traffic might get lost when the link protected LSP revert back to the primary path. PR1652651

- On PTX10008 devices, EVPN VXLAN intra-VLAN known unicast traffic gets flooded due to MAC installation failure on the Packet Forwarding Engine. PR1652876

- On PTX10008 devices, the `show snmp mib get` command returns incorrect value on jnxLED MIB OIDs. PR1654455

- On PTX10001-36MR devices, the 2x100G link fails to come up after swapping the ZR-M with LR4 DD module. PR1655180

- The protocol state synchronization on the backup Routing Engine gets affected. PR1655249

- The `UEFI BIOS Key synchronization tool - efitools.service failed` error message gets generated after the optics diagnostics test. PR1655537

- The pkid process generates core files and interfaces gets lost. PR1655949

- Incorrect transmit occurs on hardware priority when you issue the `priority medium-low` command. PR1656837

- rpm-postinst fails on boot. PR1657278

- On PTX10008 devices, the family MPLS firewall filter does not work on ingress. PR1657584

- The rpd process might crash when the BGP route resolves over another BGP route. PR1658678

- The packetio process might generate core files when the router reboots or FPC reboots. PR1658839

- The license might get out of synchronization between the primary and backup Routing Engine. PR1658869

- State gRIBI clients do not get cleaned up. PR1659442

- The configuration might roll back after you issue the `commit confirmed` command and then reboot. PR1659783

- Channelized interface might go down if you enable low-light-alarm/low-light-warning. PR1661215

- The network-instance name for streaming telemetry must be changed from default to DEFAULT to align with CONFIG stanza. PR1662999

- MVRP enabled trunk ports might go in to the `Blocked` or `Designated` state. PR1666921

- On PTX10000 devices running Junos Evolved software, the SNMP GET does not return the expected value for FPC MIBs. PR1668285

- On PTX10008 devices, the CoS process generates core files due to invalid snmp index handling missing in iterator. PR1668861

- The hardware and evo-pfemand applications might crash if idmd, fabtoken, and hardware applications get restarted immediately after a FEB offline. PR1669130

- Traffic loss might occur when multicast route changes. PR1669498

- On PTX10008 devices, the `show snmp mib walk` command fails at jnxLED mib if you perform SNMP mib walk with multiple parallel sessions. PR1669624

- Layer 2 filters matching DMAC/Etype take no effect on the Layer 2 SP-style aggregated Ethernet interface. PR1669718

- On PTX10000 devices, multicast traffic might drop. PR1669740

- On PTX10004, PTX10008, and PTX10016 devices, the transmit-rate does not achieved on queue and traffic gets dropped in the oversubscription mode. PR1670859

- Default DDOS rate limit for LLDP packets is 20,000 PPS. PR1671196

- You must not send unreplicate message to the backup during switchover. PR1671458

- On PTX10004, PTX10008, and PTX10016 devices, the evo-aftmand-bt.fpc process generates core files. PR1672512

- The new primary Routing Engine might self-reboot after the kernel crashes on an old primary Routing Engine. PR1673306

- The evo-aftmand-zx.re process generates core file at `JexprStatsGrpcCntrFarm::scan,JexprStatsOverflowMgrInst::scan,JexprStatsOverflowManager::scan,JexprStatsOverflowManager::ovfPeriodic`. PR1674724

- On PTX10003 devices, the fragment-offset-except firewall match condition does not work for the offset-1 value. PR1675482

- On PTX10004, PTX10008, and PTX10016 devices, the jnxOperatingDRAMSize value gets displayed in kilo bytes instead of bytes. PR1675811

- On PTX10000 devices, the HTTP GET fails while downloading the configuration file. PR1677231

- Fan Tray X Failure error might be seen on newer release 21.2R2. PR1652206

- After Configure rpf-check on lag interface, lag interface goes down. PR1652623

- In an SR to LDP interworking scenario, with SRMS, when a specific low privileged command is issued on an ABR rpd crashes. PR1662559

- An attacker can cause a kernel panic by sending a malformed TCP packet to the device. PR1663201

- Unexpected storage media comsumption caused by system application log. PR1677295

Infrastructure

- LLDP fails on the management interface of Junos OS Evolved platforms. PR1647923

- Configuring family MTU explicitly on an interface might cause host traffic to drop. PR1654140

- Traffic drop might occur to slow TCP reestablishment after a topology change. PR1661210

- On Junos OS Evolved platforms, there might be no connectivity between the default routing instance and other routing instance. PR1671024

Interfaces and Chassis

- The lacpd process might not come up on one of the links in the aggregated Ethernet interface bundle. PR1647145

- On PTX10003 devices, SSD DGM28-B56D81BCBQ || RE 0 SSD primary minimum supports firmware version mismatch. PR1654762

Junos XML API and Scripting

- A large configuration might not get committed at boot. PR1656436

MPLS

- The route might stay up but LSP remains down after the primary LSP interface gets administratively disabled. PR1654226

- Dynamic label space usage crosses the threshold limit of 90 percent. PR1664670

Network Management and Monitoring

- The junos-configuration-metadata.yang module does not get downloadable through CLI/Netconf. PR1643785

- The SNMP counters might get stuck. PR1663713

- The snmpd process might generate core files with filter-duplicates configuration. PR1669510

Routing Policy and Firewall Filters

- The firewalld process might crash when you use the nested filters as input list. PR1651411

- Junos OS Evolved does not support the lo0 egress filter with next-header option. PR1672315

- The aftmand process crash might be observed. PR1683361

- The aftmand process crash might be observed. PR1683361

Routing Protocols

- An error might be observed while executing a commit for the openconfig instance type. PR1644421

- Traffic loss might occur when you configure the new multicast composite next-hop. PR1651824

User Interface and Configuration

- Passwordless authentication becomes successful for configured user even after deleting the ssh public key details from the user login hierarchy. PR1625032

- Configuration archive transfer does not occur through FTP. PR1625937

- The `UI_MOTD_PROPAGATE_ERROR: Unable to propagate login announcement (motd) to /var/etc/motd.junos` syslog message gets generated, which can be ignored. PR1642743

- The ddos-protocol-group might not be listed in the ddos-protection protocols violations XML display. PR1647046

- The vlan-tagging configuration might cause the blank interface configurations after a system reboots or upgrades. PR1650151

- The l2ald process crashes when `no-persist-groups-inheritance` is configured. PR1652605

- The configd application generates core files during the configd application restart test. PR1658688

- The syslog regex matching backslash and punctuations does not filter output. PR1663346

Junos OS Evolved Release Notes for QFX5130-32CD, QFX5220, and QFX5700 Devices

IN THIS SECTION

These release notes accompany Junos OS Evolved Release 22.3R1 for QFX5130-32CD, QFX5220-32CD, QFX5220-128C, and QFX5700 switches. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

What's New

Learn about new features introduced in this release for the QFX Series switches.

Class of Service

- **Priority-based flow control X-ON Threshold and per-queue alpha support (QFX5220)**—The priority-based flow control (PFC) X-ON threshold is the ingress port's priority group (PG) shared buffer limit. At this limit, the ingress port's peer resumes transmission of packets after a brief PAUSE because of the PFC message sent by this ingress port. You can tune globally the limit of buffers that each queue can consume from the shared pool based on the dynamic threshold setting called the *alpha value*. Starting with Junos OS Evolved 22.3R1 on QFX5220 devices, you can fine tune the X-ON threshold through the congestion notification profile (CNP) and fine tune the alpha value on a per-queue basis through a scheduler.

  [See xon (Input Congestion Notification) and buffer-dynamic-threshold .]

EVPN

- **EVPN-VXLAN fabric with an IPv6 underlay (QFX5130-32CD and QFX5700)**—Starting in Junos OS Evolved Release 22.3R1, you can configure an EVPN-VXLAN fabric with an IPv6 underlay. We support this feature with all service types in MAC-VRF routing instances. You can configure either an IPv4 or an IPv6 underlay across the EVPN instances in the fabric. You can't mix IPv4 and IPv6 underlays in the same fabric.

  To enable this feature, configure the underlay VXLAN tunnel endpoint (VTEP) source interface in the MAC-VRF instance as an IPv6 address. Also assign IPv6 addresses on the EVPN core-facing

interfaces so the devices can reach each other using IPv6. However, you must use the IPv4 loopback address as the router ID for BGP handshaking to work.

[See EVPN-VXLAN with an IPv6 Underlay and Example: Configure an IPv6 Underlay for Layer 2 VXLAN Gateway Leaf Devices.]

Flow-based and Packet-based Processing

- **Support for Dynamic Load-Balancing (QFX5130-32CD and QFX5700)**—Starting in Junos OS Evolved Release 22.3R1, QFX5130-32CD and QFX5700 switches support Dynamic Load-Balancing (DLB) for equal-cost multipath (ECMP) and link aggregation group (LAG). DLB is an enhancement to static load balancing. DLB considers member bandwidth utilization along with packet content for member selection.

  You can use the following DLB modes to load-balance traffic:

  - Flowlet

  - Assigned flow

  - Per-packet

  To configure DLB for ECMP, include the `ecmp-dlb` statement at the [`edit forwarding-options enhanced-hash-key`] hierarchy level.

  To configure DLB for LAG, include the `dlb` statement at the [`edit interfaces aex aggregated-ether-options`] hierarchy level.

  > (i) **NOTE**: When you configure both DLB and resilient hashing at the same time, a commit error occurs.

Interfaces

- **Support for 8x50G DAC optics (QFX5130-32CD and QFX5220-32CD)**—Starting in Junos OS Evolved Release 22.3R1, we support 8x50G DAC 1M, 2M, 2.5M, and 3M variant optics. You can channelize every second port. Note that if you channelize one port, you must mark the next port as unused.

  [See QFX5220-32D guide.]

Junos Telemetry Interface

- **Telemetry support for CoS ingress packet drop accounting (QFX5220)**—Junos OS Evolved Release 22.3R1 introduces telemetry support to account for packets that are dropped because of ingress port congestion. Counters for priority flow control (PFC), explicit congestion notification (ECN), and ingress drops are exported using the sensor **/junos/system/linecard/interface/traffic**. Counters for

PFC, ECN, and ingress drops are also exported using OpenConfig sensor **/interfaces/interface/**. Priority group (PG) buffer utilization is exported using the sensor **/junos/system/linecard/qmon-sw/**.

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

Multicast

- **Support for MC-LAGs (QFX5220)**—Starting in Junos OS Evolved Release 22.3R1, QFX5220 switches support multichassis link aggregation groups (MC-LAGs). The switches support the following features:

  - eBGP/OSPF routing protocol (IPV4)

  - DHCP (IPV4)

  - Layer 2 bridging for active-active mode

  - Layer 3 unicast with VRRP (IPV4)

  - Layer 3 VPN (IPV4, only on core side)

  [See Understanding Multichassis Link Aggregation Groups.]

Routing Protocols

- **Maximum reference bandwidth increased to 4 TB for IGP protocols (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016, QFX5130-32CD, QFX5700, and QFX5220)**—Starting with Junos OS Evolved Release 22.3R1, we've increased the maximum reference bandwidth for IS-IS and OSPF interior gateway protocol (IGP) protocols from 1 Tbps to 4 Tbps. The default bandwidth is 100 Mbps. You can increase the reference bandwidth to adjust the path metrics, which you use to determine the preferred path in case of multiple equal-cost routes to a destination.

  To configure the reference bandwidth, use the `reference-bandwidth` *reference-bandwidth* statement at the `[edit protocols isis]` hierarchy level or the `[edit protocols (ospf | ospf3)]` hierarchy level.

  [See reference-bandwidth (Protocols IS-IS) and reference-bandwidth (Protocols OSPF).]

- **Support for BGP flowspec (QFX5130-32CD and QFX5220)**—Starting with Junos OS Evolved Release 22.3R1, we support traffic flow specification, a distributed denial of service (DDoS) mitigation solution that provides traffic filtering and rate-limiting capabilities. A BGP speaking device identifies packets that match conditions defined in a flow specification. The device distributes these packets according to the listed actions.

  [See Understanding BGP Flow Routes for Traffic Filtering.]

- **Fast lookup of origin and neighbor ASs (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10004, PTX10008, PTX10016, QFX5130-32CD, QFX5700, and QFX5220)**—Starting in Junos

OS Evolved Release 22.3R1, you can use the new `asregex-optimize` configuration statement at the `[edit policy-options defaults]` hierarchy level to perform a fast lookup of origin and neighbor autonomous systems (ASs). The `asregex-optimize` configuration statement is not enabled by default.

[See Improve the Performance of AS Path Lookup in BGP Policy.]

- **Sharding support for conditional route manager (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and QFX5130-32CD)**—Starting in Junos OS Evolved Release 22.3R1, we support sharding for conditional route manager to fetch active route information from the main thread for conditions. Using this approach, the condition manager on the shard interacts with the route target (RT) proxy client to get active route information. The condition manager on the main thread interacts with the RT proxy server to send details to shards. The condition manager on shards stores active route information that is TRUE or FALSE for any condition and evaluates policy (having the condition) based on that. No change in the condition manager occurs on the main thread with respect to route lookup, flash mechanism, or dependent route operations such as additions or deletions.

  We have updated the following command outputs:

  - `show policy condition`

  - `show policy condition detail`

  - `show policy condition <condition-name>`

  - `show policy condition <condition-name> detail`

  - `show policy condition rib-sharding <shard-name>`

  - `show policy condition detail rib-sharding <shard-name>`

  - `show policy condition <condition-name> rib-sharding <shard-name>`

  - `show policy condition <condition-name> detail rib-sharding <shard-name>`

  [See Routing Policy Match Conditions, rib-sharding, and show policy conditions.]

- **Strip/replace BGP private-AS support (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10004, PTX10008, PTX10016, QFX5130-32CD, QFX5130-48C, QFX5700, and QFX5220)**—Starting in Junos OS Evolved Release 22.3R1, we have introduced the `strip-as-path` policy option. This policy option removes the incoming Autonomous System (AS) path, AS_PATH, as part of the import policy for a BGP session. This policy option also replaces the received AS_PATH with the receiving router's local-AS number for the receiving session. Note that the local-AS number may be different from the number configured under the autonomous-system at the `[edit routing-options]` hierarchy level.

If you need to normalize externally injected routes, you can use this policy option for the incoming AS_PATH so that it can be used similarly to routes that originate solely within the fabric. The new `strip-as-path` policy option has no impact on the BGP export policy.

You can configure the `strip-as-path` option from the policy-options `then` clause:

```
set policy-options policy-statement do-strip term a then strip-as-path
```

[See Autonomous Systems for BGP Sessions.]

- **Origin validation communities conversion to keywords (PTX10001-36MR, PTX10008, PTX10016, QFX5130-32CD, and QFX5220)**—Starting in Junos OS Release Evolved 22.3R1, you can choose to accept or reject the origin validation extended communities received from an external BGP (EBGP) peer. The default behavior of Origin Validation State Extended Community (OVS EC) is changed to rejected if received from an EBGP peer. You can configure OVS EC to accept the community when needed. We also support the configuration of distinguished communities with keywords (valid, invalid, and unknown) at all the three layers of the BGP configuration hierarchy: global, group, and per-neighbor. If you enable the OVS EC at a hierarchy level, it's enabled for the lower levels as well. However, you can choose to disable it explicitly at a lower layer if required in any instance.

  To accept origin validation communities from an EBGP peer, use `origin-validation accept` at the [`edit protocols bgp ebgp-community-cleanup`], `edit protocols bgp group <group-name> ebgp-community-cleanup`], or [`edit protocols bgp group <group-name> neighbor <address> ebgp-community-cleanup`] hierarchy level.

  To reject origin validation communities from an EBGP peer, use `origin-validation reject` at the [`edit protocols bgp ebgp-community-cleanup`], `edit protocols bgp group <group-name> ebgp-community-cleanup`], or [`edit protocols bgp group <group-name> neighbor <address> ebgp-community-cleanup`] hierarchy level.

  [See BGP Origin Validation.]

Additional Features

We have extended support for the following features to these platforms:

- **Controller-based BGP multicast signaling** (PTX10001-36MR, PTX10004, PTX10008, and QFX5220)

  [See Controller-Based BGP Multicast Signaling.]

- **Enhanced rapid ping command output (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016,QFX5130-32CD, QFX5220, and QFX5700)**— Output for ping commands using the rapid option now displays the following symbols:

  - "!" for echo reply packets received within 500 ms

  - "." for echo reply packets not seen within 500 ms

  - "C" for received responses where the checksum of the reply is bad

[See ping.]

- **Filter-based forwarding (FBF) support on L3 sub-interfaces** (QFX5700)

  - FBF on AE and non-AE interfaces

  - FBF on VXLAN-enabled L3 sub-interfaces

  - FBF on IRB interfaces

  If a filter has terms with routing-instance action, only the terms with routing-instance actions will be processed at a higher priority compared to other terms in the filter. Suppose that the filter has term1 without routing-instance action and term2 with routing-instance action: If a packet matches both term1 and term2, then term2 will take a higher priority compared to term1. Therefore, the actions of term2 will be applied.

  [See Filter-Based Forwarding Overview.]

- **MLD snooping and IRB stitching support** (QFX5130-32CD, QFX5220, and QFX5700)

  [See Understanding MLD Snooping.]

- **Media Access Control Security (MACsec) (QFX5700 with 16x100G line cards)**

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

- **Operational command RPC support for returning JSON and XML output in minified format in NETCONF sessions (ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016, QFX5130-32CD, and QFX5220)**

  [See Specifying the Output Format for Operational Information Requests in a NETCONF Session.]

- **Support for the NTP restrict command** (ACX7509, PTX10004, PTX10016, and QFX5700)

  [See Configuring NTP Access Restrictions for a Specific Address (SRC CLI).]

- **Supported transceivers, optical interfaces, and DAC cables**—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update this tool and provide the first supported release information when the optic becomes available.

What's Changed

Learn about what changed in these releases for QFX Series switches.

What's Changed in Release 22.3R1-S2

Junos XML API and Scripting

- The `file copy` command supports only text-formatted output in the CLI (ACX Series, PTX Series, and QFX Series)—The `file copy` command does not emit output when the operation is successful and supports only text-formatted output when an error occurs. The `file copy` command does not support using the `| display xml` filter or the `| display json` filter to display command output in XML or JSON format in any release. We've removed these options from the CLI.

What's Changed in Release 22.3R1

Learn about what changed in these releases for QFX Series switches.

Authentication and Access Control

- **Enhanced SSH hostkey algorithm configuration**—We've introduced the `hostkey-algorithm-list` statement at the [`edit system services ssh`] hierarchy level. This enhancement enables you to configure only the specified SSH hostkey algorithms. The system disables the remaining unspecified hostkey algorithms. In earlier releases, you need to disable the hostkey algorithms explicitly. All the hostkey algorithms at this hierarchy enabled by default. The DSS algorithm is no longer available at this new hierarchy.

  In addition, we've deprecated the `hostkey-algorithm` statement at the [`edit system services ssh`] hierarchy level.

  [See hostkey-algorithm.]

EVPN

- **AR replicators with OISM install multicast states only on the OISM SBD (QFX5130-32CD and QFX5700)**—In an EVPN-VXLAN ERB fabric with many VLANs, QFX5130-32CD and QFX5700 switches running as assisted replication (AR) replicators with optimized intersubnet multicast (OISM) might have scaling issues when they install multicast (*,G) states (with IGMPv2) or (S,G) states (with IGMPv3). As a result, these switches only install these multicast states on the OISM supplemental bridge domain (SBD) VLAN. They don't install these states on all OISM revenue bridge domain VLANs. On those devices, you see multicast group routes only on the SBD in `show multicast snooping route` command output.

  [See OISM and AR Scaling with Many VLANs.]

General Routing

- Starting in Junos OS Evolved Releases 22.1R3, 22.2R2, and 22.3R1, QFX5130 switches don't copy the Type of Service (ToS) field when encapsulating a VXLAN packet by default. You can enable copying the ToS field upon VXLAN encapsulation using the vxlan-tos-copy-filter statement at the **edit forwarding-options** hierarchy. This statement copies both the DSCP and ECN values in the ToS field from the IP header of a packet to the outer IP header of the VXLAN packet.

- **Instance type change is not permitted from default to L3VRF in open configuration (ACX Series and QFX Series)**—DEFAULT_INSTANCE is the primary instance that runs when there is no specific instance type configured in the route `set routing-options?`. Any instance you explicitly configure is translated into `set routing-instance r1 routing-options?`. The issue appears in translation, when you change instance type DEFAULT_INSTANCE (any instance to DEFAULT_INSTANCE) to L3VRF or L3VRF to DEFAULT_INSTANCE. As a result, such changes are not permitted. Additionally, DEFAULT_INSTANCE can only be named DEFAULT, and DEFAULT is reserved for DEFAULT_INSTANCE, therefore allowing no such changes.

- Prior to this change when route sharding is configured the output of CLI `show route` commands included information about sharding. After the change the use must add the **rib-sharding all** argument to CLI `show route` commands to display sharding information.

- **sFlow configuration**— sFlow configuration is allowed only on et, xe, and ge interfaces in EVO-based platforms. All other interfaces are blocked for configuring sFlow on EVO platforms. A cli error will be thrown if sFlow is configured on any other interface other than et, xe or ge interface.

- The traffic rate could display incorrect values in the `show services inline ip-reassembly statistics fpc x pfe-slot y` output.

Juniper Extension Toolkit (JET)

- **Python 3 is the default and only Python version for executing Juniper Extension Toolkit Python scripts (ACX Series, PTX Series, and QFX Series)**—Junos OS Evolved supports only Python 3 for executing Juniper Extension Toolkit (JET) scripts written in Python. Python 2.7 is no longer supported for executing JET scripts, and we've deprecated the `language python` statement at the `[edit system scripts]` hierarchy level.

  [See Understanding Python Automation Scripts for Junos Devices.]

Junos XML API and Scripting

- **Deprecated functions in the `libpyvrf` Python module (ACX Series, PTX Series, and QFX Series)**—The `libpyvrf`Python module no longer supports the `get_task_vrf()` and `set_task_vrf()` functions.

[See How to Specify the Routing Instance in Python 3 Applications on Devices Running Junos OS Evolved.]

- **Python 3 is the default and only Python version for executing commit, event, op, and SNMP Python scripts (ACX Series, PTX Series, and QFX Series)**—Junos OS Evolved supports only Python 3 for executing commit, event, op, and SNMP scripts written in Python. Python 2.7 is no longer supported for executing these types of scripts, and we've deprecated the `language python` statement at the `[edit system scripts]` hierarchy level.

  [See Understanding Python Automation Scripts for Junos Devices.]

MPLS

- Starting with Junos OS and Junos Evolved release 21.4R3 a CSPF LSP uses a new instance ID when attempting to re-signal a down LSP.

- **Display flexible algorithm information for SRv6 locators in TED database**—Use the `show ted database extensive` command to view the metric, flags, and flexible algorithm information associated with a SRv6 locator. Prior to this release, this information was not included in the TED database.

  [See show ted database.]

Network Management and Monitoring

- **Python 3 is the default and only Python version for executing YANG action and translation Python scripts (ACX Series, PTX Series, and QFX Series)**—Junos OS Evolved supports only Python 3 for executing YANG action and translation scripts written in Python. Python 2.7 is no longer supported for executing YANG action and translation scripts, and we've deprecated the `language python` statement at the `[edit system scripts]` hierarchy level.

  [See Understanding Python Automation Scripts for Junos Devices.]

- **Enhancement to the jnxRmonAlarmState (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series)**—You can now view the following additional values for the jnxRmonAlarmState when you use the show snmp mib walk jnxRmonAlarmTable: fallingThreshold (6) - If the value is less than or equal to falling-threshold risingThreshold (5) - If the value is greater than or equal to rising-threshold getFailure (7)- If the value is any value other than noError for the current internal 'get' request In earlier releases, you could view only the following status for the jnxRmonAlarmState: unknown (1), underCreation (2), or active (3).

OpenConfig

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

Platform and Infrastructure

- **Enhanced bandwidth and burst policer value**—We've updated the default bandwidth value from 20000 to 100 pps and burst policer value from 20000 to 100 packets. This enhancement avoids the CPU usage of `eventd` and `snmpd` reaching more than 100%. Earlier to this release, when the system receives a violated traffic for SNMP along with other protocols traffic, the CPU usage of `eventd` and `snmpd` was reaching more than 100% with an error.

  [See show ddos-protection protocols parameters.]

- Starting Junos Evolved release 22.3R1, support is provided to limit Network Time Protocol (NTP) configuration to one address family (inet vs inet6). You can configure one source-address per inet and inet6 family for each routing-instance in NTP. For example, the following configuration is valid: `set system ntp source-address 2620:149:1d06:100::1 set system ntp source-address 10.10.10.100`.

System Management

- **Command to automate SSH key-based authentication (ACX Series, PTX Series, and QFX Series)**—You can set up SSH-key based authentication between the network device and a remote host by issuing the `request security ssh password-less-authentication` operational mode command. When you execute the command with the appropriate options, the device generates SSH keys for the current user, provided the user does not already have existing keys, and transfers the user's public key to the **authorized_keys** file of the specified user on the remote host.

  [See request security ssh password-less-authentication.]

Timing and Synchronization

- **Performance monitoring time interval with UTC on Junos OS Evolved platforms** —The performance monitoring (PM) time interval for 1-day bins on Junos OS Evolved platforms begins at midnight in the UTC zone, aligning with the standard behaviour of Junos OS. This synchronization allows you to maintain consistent performance monitoring schedules across platforms, enhancing the accuracy and reliability of network performance data.

User Interface and Configuration

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

  [See temperature-sensor.]

- **Persistent CLI timestamps**—To have a persistent CLI timestamp for the user currently logged in, enable the `set cli timestamp` operational command. This ensures the timestamp shows persistently for each new line of each SSH session for the user or class until the configuration is removed. To enable timestamp for a particular class with permissions and format for different users, configure the following statements:

```
set system login class class name permissions permissions
set system login class class name cli timestamp set system login user username class class
name authentication plain-text-password
```

> **NOTE**: The default timestamp format is %b %d %T. You can modify the format per your requirements. For example, you can configure the following statement:
>
> `set system login class class name cli timestamp format "%T %b %d`

To enable timestamp for a particular user with default class permissions and format, configure the following statements:

```
set system login user username class class name authentication plain-text-password
set system login user username cli timestamp
```

Known Limitations

IN THIS SECTION

- General Routing | **89**

Learn about limitations in this release for the QFX Series switches.

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

General Routing

- On QFX5220-32CD, VLANs between 3968 and 4095 are reserved for Layer 3 interfaces by default. So, these VLANs cannot be used for Layer 2 interfaces. There is no `commit check` added for this purpose. You need to take care of this while configuring VLANs for Layer 2. PR1423468

- QFX5220-128C :: Tx laser disabled alarm or Rx loss of signal alarm do not turn on or off as expected. Takes long time when Local or remote interface is disabled or enabled.PR1661939

Open Issues

IN THIS SECTION

Learn about open issues in this release for QFX Series switches.

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

General Routing

- On the QFX5130-32CD platform running Junos OS Evolved, you cannot clear or reset the disk option specified in the scheduled `request node reboot` command. The node reboots with the disk option last specified. PR1517596

- On QFX5700, 400G DAC flap might be seen after OIR, FPC restart, device reboot enabling or disabling interface.PR1618488

- On QFX5700, ungraceful removal (OIR) of FPC or an FPC fault might result in a PCIE MAJOR alarm **PCI Uncorrected error on dev 0000:00:03.0** which does not get cleared. The only way to clear this alarm is reboot of the device. There are 2 situations in which this alarm can be seen:

  1. **FPC is faulty**: In rare FPC fault cases, the PCI Uncorrected error alarm might be seen along with FPC going to a Fault state as indicated by the `show chassis fpc` command. This is accompanied by

other FPC major alarms. Once the faulty FPC is replaced with a good one, the alarm is still seen, and a reboot is required to clear this alarm. Post identification of the fault and FPC replacement, this alarm is harmless, and FPC state can be confirmed through the `show chassis fpc` command.

2. **Ungraceful OIR**: The ungraceful removal of FPCs is not recommended on QFX5700. This operation might result in PCI Uncorrected Error alarm.

Use one of the following two methods to do a graceful FPC OIR removal:

- Execute the `request chassis fpc slot <slot > offline` command from the CLI.

- Press the Offline Button for 1 second on the FPC to offline the FPC. Once the FPC is gracefully offlined both LEDs - PWR and STS go off. The FPC can be removed at this point.

  PR1620197

- 400G LR4-10 link does not come up after deleting `interface disable` configuration when port is disabled followed by system reboot. PR1625494

- In Junos OS Evolved Release 22.3R1, OSPF and BGP sessions over an IRB interface do not work for EVPN VXLAN deployments. PR1688681

User Interface and Configuration

- The system might ask for your password when you are trying to save configuration file. PR1665008

- [ISSU] [default] QFX5220-32CD and QFX5220-128C :: JDI_REG_FT_REGRESSIONS:: ISSU is not successful on a device loaded with Junos OS Evolved 22.3 latest ci passed build - SSH failure after ISSU. PR1679476

Resolved Issues

IN THIS SECTION

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

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

General Routing

- In scaled Layer 2 network, error logs are printed for MAC Creation. MAC learning works as expected. PR1491933

- On QFX5700 platforms few interfaces do not come up after removing channelization through single commit, that is by using `delete interfaces`. PR1592238

- Unified led scheme for QFX5220 or QFX5130. PR1616209

- QFX5220-128C : MDIO forward download fails after image upgrade. PR1636181

- QFX5220 platform might experience system reboot or shutdown in rare cases. PR1638961

- After sigkill or app crash, jstatsd app does not come up. PR1641229

- FEC corrected errors which are cleared with `clear statistics` command show up as huge value after unified ISSU. PR1641583

- QFX5130-32CD, QFX5220-32CD : Unexpected carrier transitions are seen on JNP-100G-2X50G-xM after plug out and plug in. PR1642744

- Non standard optics causes pcid core file generation issue. PR1649925

- QFX5130: A few MACS are missing from `show ethernet-switching table`. PR1650329

- Junos OS Evolved QFX **EvoPfemand-main** process memory leak. PR1652873

- TOS(DSCP+ECN) bits does not get copied from the inner Layer 3 header to outer VXLAN header. PR1658142

- Junos OS Evolved white space in optics serial number in `show chassis hardware display xml or json`. PR1665229

- QFX5130 sends a flow sample with the wrong value of flow record in sflow sampled packet. PR1666434

- TPI-101526 :Junos OS Evolved:QFX5700 : 100% Layer 2 MAC traffic is not forwarded to the CE interfaces from the core on QFX5700. PR1668921

- On QFX5130-32CD and QFX5700 platforms, IPv6 neighborships fail to establish if IPv6 loopback filters are configured. PR1671730

- The interface does not come back to default port speed when ZTP is aborted. PR1672101

Infrastructure

- QFX5220: Change in the output for L3VPN.inet6 route table in `show route forwarding-table summary | display xml` command.PR1653182

Routing Protocols

- `show multicast snooping route extensive instance evpn-vxlan-A` with vlan filter does not show VE,AR mesh group route entries. PR1649410

User Interface and Configuration

- The vlan-tagging configuration might cause blank interface configuration after a system reboot or upgrade. PR1650151

Upgrade Your Junos OS Evolved Software

Products impacted: ACX7024, ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016, QFX5130-32CD, QFX5220-32CD, QFX5220-128C, and QFX5700.

Follow these steps to upgrade your Junos OS Evolved software:

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. In the Find a Product box, enter the Junos OS platform for the software that you want to download.

3. Select Junos OS Evolved from the OS drop-down list.

4. Select the relevant release number from the Version drop-down list.

5. In the **Install Package** section, 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 device or to your internal software distribution site.

10. Install the new 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.

For more information about software installation and upgrade, see Software Installation and Upgrade Overview (Junos OS Evolved). For more information about EOL releases and to review a list of EOL releases, see https://support.juniper.net/support/eol/software/junosevo/.

Licensing

In 2020, Juniper Networks introduced a new software licensing model. The Juniper Flex Program comprises a framework, a set of policies, and various tools that help unify and thereby simplify the multiple product-driven licensing and packaging approaches that Juniper Networks has developed over the past several years.

The major components of the framework are:

- A focus on customer segments (enterprise, service provider, and cloud) and use cases for Juniper Networks hardware and software products.

- The introduction of a common three-tiered model (standard, advanced, and premium) for all Juniper Networks software products.

- The introduction of subscription licenses and subscription portability for all Juniper Networks products, including Junos OS and Contrail.

For information about the list of supported products, see Juniper Flex Program.

Finding More Information

- **Feature Explorer**—Juniper Networks Feature Explorer helps you to explore software feature information to find the right software release and product for your network.

  https://apps.juniper.net/feature-explorer/

- **PR Search Tool**—Keep track of the latest and additional information about Junos OS open defects and issues resolved.

  https://prsearch.juniper.net/InfoCenter/index?page=prsearch

- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms.

  https://apps.juniper.net/hct/home

  > (i) **NOTE**: To obtain information about the components that are supported on the devices and the special compatibility guidelines with the release, see the Hardware Guide for the product.

- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6.

  https://pathfinder.juniper.net/compliance/

Requesting Technical Support

IN THIS SECTION

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.

- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.

- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/

- Search for known bugs: https://prsearch.juniper.net/

- Find product documentation: https://www.juniper.net/documentation/

- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/

- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/

- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

Revision History

28 March 2025—Revision 15, Junos OS Release 22.3R1

24 September 2024—Revision 14, Junos OS Release 22.3R1

4 July 2024—Revision 13, Junos OS Release 22.3R1

30 May 2024—Revision 12, Junos OS Release 22.3R1

22 February 2024—Revision 11, Junos OS Release 22.3R1

10 August 2023—Revision 10, Junos OS Release 22.3R1

20 July 2023—Revision 9, Junos OS Release 22.3R1

15 June 2023—Revision 8, Junos OS Release 22.3R1

2 March 2023—Revision 7, Junos OS Release 22.3R1

2 February 2023—Revision 6, Junos OS Release 22.3R1

24 November 2022—Revision 5, Junos OS Release 22.3R1

20 October 2022—Revision 4, Junos OS Release 22.3R1

7 October 2022—Revision 3, Junos OS Release 22.3R1

26 September 2022—Revision 2, Junos OS Release 22.3R1

22 September 2022—Revision 1, Junos OS Release 22.3R1