Release Notes

Published
2026-01-08

Junos OS Evolved Release 24.2R1

Introduction

Use these release notes to find new and updated features, software limitations, and open issues for Junos OS Evolved Release 24.2R1.

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

Table of Contents

Junos OS Evolved Release Notes for ACX Series

IN THIS SECTION

These release notes accompany Junos OS Evolved Release 24.2R1 for ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348 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 24.2R1, click the Group by Release link. You can collapse and expand the list as needed.

- ACX7024
- ACX7024X
- ACX7100-32C
- ACX7348
- ACX7100-48L
- ACX7509

The following sections highlight the key features in this release.

Hardware

- **ACX7332 router (ACX Series)**—We introduce the Juniper Networks® ACX7332 Cloud Metro Router, an extended temperature-rated (E-Temp) platform from the ACX7300 series that supports a variety of deployment scenarios. With a compact 3-RU semi-modular form factor, it offers an aggregation solution that gives cloud providers and service providers the performance and scalability needed as networks grow.

  The ACX7332 router provides 1-Gigabit Ethernet (GbE) through 400GbE port flexibility and a throughput of 2.4 Tbps. The router has a fixed FPC with thirty-two 25GbE and eight 100GbE ports, dual Routing Engines, three bays for pluggable interface modules, redundant power supply modules (AC or DC), and four fan trays (two fans per tray).

  The ACX7332 router supports the following pluggable FPCs:

- ACX7K3-FPC-2CD4C—Two 400GbE and four 100GbE ports
- ACX7K3-FPC-16Y—Sixteen 50GbE ports

The ACX7332 router runs Junos OS Evolved and provides several capabilities that include support for the latest protocol and traffic engineering technologies, enhanced security, and precision timing for mobile backhaul applications. These capabilities and features enable you to create converged, virtualized, and automated architectures to address the rapid growth of 5G, IoT, and the cloud.

Table 1: ACX7332 Feature Support

Feature	Description
Authentication and Access Control	• Support for 802.1X authentication on Layer 2 and Layer 3 interfaces. [See 802.1X Authentication on Layer 2 Interfaces.]

Chassis	• Supports two Routing Engines, one Control Board, one Forwarding Engine Board (FEB), one fixed FPC, and three removable FPCs chassis supports:
	  • Platform FEB and FPC FRU presence and power-up.
	  • Infrastructure databases and services.
	  • Power management.
	  • Environment monitoring and cooling.
	  • System LED behavior.
	• Platform resiliency support for device chassis, RCB, PSM, fan tray, input, and output devices.

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
Class of service	• Support for classification and rewrite rules of all types (Inet-Prec/DSCP/DSCP-v6/IEEE-802.1p/IEEE-802.1ad) at the logical interface level. Supports logical interfaces classification and rewrite rules for MPLS, VPLS, Layer 3 VPN, Layer 2 circuit, CCC, IRB, and EVPN. [See Classifiers and Rewrite Rules at the Global, Physical, and Logical Interface Levels Overview.] • Support for port shaping and scheduling with eight VoQ queues per port and two scheduling priority levels (strict-high and low). Supports multiple strict-high priority queues (RR scheduling), multiple low-priority queues (WFQ scheduling), low latency queues (LLQ), and default deep buffers. [See Schedulers Overview for ACX Series Routers and Shared and Dedicated Buffer Memory Pools on ACX Series Routers .] • Support for hierarchical class of service (CoS). Hierarchical CoS support for Layer 3 VPN, Layer 2 VPN, Layer 2 Circuit, VPLS, and EVPN services. [See Hierarchical Class of Service in ACX Series Routers.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

Dynamic Host Configuration Protocol	• DHCP server and DHCP relay configuration for IPv4 and IPv6 services.
	
	[See DHCP Overview.]
	
	• DHCP relay deployment of EVPN over MPLS, which includes:
	
	  • Edge-routed bridging (ERB)—Edge model where DHCP clients are connected and relayed in network leaf devices. The spine PEs do not perform DHCP relay functions, and the routers support transit spine functionality running protocols such as BGP for integrated routing and bridging (IRB).
	
	• The following functionalities:
	
	  • EVPN over MPLS Ethernet-LAN
	
	  • DHCPv4 and DHCPv6 relay options
	
	  • Stateless forward-only mode for DHCP relay over VPN
	
	  • Anycast IP address with IRB for a relay source
	
	  • Client VRFs only
	
	• DHCPv4 and DHCPv6 relay agent support for MC-LAG. DHCP relay agent support includes:
	
	  • DHCPv4 and DHCPv6 stateless forward-only option on Layer 3 static interfaces over MC-LAG.
	
	  • DHCPv4 and DHCPv6 stateless forward-only option on IRB interfaces over MC-LAG.
	
	  • DHCPv4 and DHCPv6 forward-snooped-clients on dual-stack configurations.
	
	[See DHCP Relay Agent and Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent.]
	
	[See DHCP Relay Agent in EVPN-MPLS Network.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

EVPN	• Support for 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 networks with ECMP and Fast Reroute (FRR)
	  • Control-word support for EVPN
	  • EVPN Proxy Address Resolution Protocol (ARP) and ARP suppression
	  • EVPN-ELAN over segment routing
	  [See EVPN Feature Guide.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

	• Virtual private wire service (VPWS) with EVPN signaling mechanisms and flexible cross-connect support.
	
	[See Overview of VPWS with EVPN Signaling Mechanisms.]
	
	• EVPN E-LAN active-active multihoming with EVPN aliasing support for ESI LAG.
	
	[See Example: Configuring EVPN Active-Active Multihoming.]
	
	• All-active multihoming redundancy in both Ethernet VPNvirtual private wire service (EVPN-VPWS) and EVPN-VPWS with flexible cross-connect.
	
	[See Overview of Flexible Cross-Connect Support on VPWS with EVPN.]
	
	• EVPN VPWS multihoming all-active forsegment routing over MPLS
	
	[See Overview of VPWS with EVPN Signaling Mechanisms.]
	
	• Entropy and flow label for EVPN-ELAN
	
	[See Configuring Entropy Labels.]
	
	• Support for the following EVPN-MPLS features:
	
	  • 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

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
	• 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 the following EVPN-VPWS features: • EVPN-VPWS FXC VLAN unaware service • EVPN-VPWS FXC VLAN aware service • EVPN-VPWS over segment routing • Single homing and all active multihoming support • Flow-aware transport (FAT) pseudowire labels • Entropy labels [See Overview of VPWS with EVPN Signaling Mechanisms.]
Firewall filters	• Support for firewall filters and policers. You can configure firewall filters with packet match conditions for the bridge domain, IPv4, IPv6, CCC, and MPLS families. In addition to packet match conditions, the count, discard, log, syslog, and policer actions are supported. [See Standard Firewall Filter Match Conditions and Actions on ACX Series Routers Overview.] • Filter-based forwarding (FBF). [See Filter-Based Forwarding Overview.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
	• Firewall filter protocols: MPLS, CCC, virtual private LAN service (VPLS), and ANY. [See Firewall Filters Overview, Filter-Based Forwarding Overview, Understanding Filter-Based Forwarding to a Specific Outgoing Interface or Destination IP Address, and Guidelines for gRPC and gNMI Services.]
High availability	• VRRP for IPv4 and IPv6. [See VRRP and VRRP for IPv6 Overview.] • BFD over label-switched paths (LSPs) or RSVP-based LSPs in a centralized mode. [See Bidirectional Forwarding Detection (BFD) for MPLS.] • High availability on these routers are supported at the hardware level. Graceful routing engine switchover is not supported in this release. • Support for loop-free alternate (LFA) routes for OSPF and IS-IS. LFA enables IP fast-reroute capability for OSPF and IS-IS. [See Loop-Free Alternate Routes for OSPF Overview and Understanding Loop-Free Alternate Routes for IS-IS.] • BFD-triggered fast reroute for unicast next hops. [See Bidirectional Forwarding Detection (BFD) for MPLS, session-id-change-limiter-indirect, and no-bfd-triggered-local-repair.]
Interfaces	• The ACX7332 router provides 1GbE through 400GbE port flexibility and a throughput of 2.4 Tbps. [See Port Speed.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

	• Support for 6xQSFPDD and 16xSFP56 FPC line cards. The 6xQSFPDD FPC Line Card has two QSFPDD ports (Port 0 and 2) and four QSFP ports (Port 1, 3, 4 and 5). The 16xSFP56 FPC line card has 16 SFP56 ports (Port 0 to 15). Slot 1 and 2 supports 10-Gbps, 25-Gbps, and 50-Gbps speeds. Slot 3 supports 1-Gbps, 10-Gbps, and 25-Gbps speeds.
	
	[See Port Speed.]
	
	• Support for LACP link protection. We support 1:1 and N:N link protection.
	
	[See link-protection.]
	
	• Resiliency support for ASIC error and CM infra. Resiliency only supports logging and detection and not action.
	
	• Features supported for unnumbered interfaces:
	  • Bidirectional Forwarding Detection (BFD)
	  • BGP labeled unicast
	  • Ethernet VPN virtual private wire service (EVPN-VPWS)
	  • IS-IS protocol adjacency
	  • Label Distribution Protocol (LDP)
	  • Layer 2 VPN and Layer 2 circuit
	  • Layer 3 VPN
	  • Qualified next hop
	  • RSVP-TE
	  • Static subnet route
	  • Source Packet Routing in Networking (SPRING) over OSPFv2

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
	• SPRING-TE • Segment routing with MPLS • Static LSP • Source Packet Routing in Networking (SPRING) over OSPFv2 • SPRING-TE • Segment routing with MPLS • Static LSP [See Configure unnumbered Interfaces.]
Junos Telemetry Interface (JTI)	• Logical subinterface and Packet Forwarding Engine drop, pipe, and line-card counter sensor support for JTI. [See Junos YANG Data Model Explorer.] • Support for telemetry interfaces.
Layer 2 features	• Ethernet ring protection switching (ERPS) with G.8032 version 2. [See Understanding Ethernet Ring Protection Switching Functionality .] • Support for the following advanced Layer 2 (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

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

	• MAC learning, ageing, and limiting
	• Single-learning domain per bridge domain
	• 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
	  • For family `inet6`, Layer 3 destination and source addresses
	  • For family `inet6`, Layer 4 destination and source ports

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

	• Encapsulation types:
	  • `extended-vlan-bridge`
	  • `vlan-bridge`
	  • `ethernet-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.]
	• Layer 2 protocol tunneling (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.
	• Storm control.
	[See Understanding Storm Control.]
	• Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP).
	[See Spanning-Tree Protocol Overview.]
	• MAC move limit and multiple trunk ports, virtual private LAN service (VPLS), and EVPN networks.
	[See Understanding MAC Limiting and MAC Move Limiting.]
	• Layer 2 Control Protocol (L2CP) BPDUs are transparently forwarded in hardware unless a specific protocol is configured on the incoming interface. This feature helps you to configure and enable L2PT.
	• VLAN sensor support.

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

	[See Telemetry Sensor Explorer.]
	
	[See Understanding Layer 2 Bridge Domains on ACX Series and Q-in-Q Tunneling on ACX Series, Bridging and VLANs, and Configuring MAC Address Flooding and Learning for VPLS .]
	
	• Multichassis link aggregation groups (MC-LAGs). The following Layer 2 features are available on MC-LAGs:
	  • Layer 2 bridging for active-active and active-standby modes
	  • Layer 2 unicast with and without IGMP snooping
	  • Layer 3 unicast with and without IGMP snooping
	  • Layer 2 multicast with and without IGMP or MLD snooping
	  • Layer 3 multicast with and without IGMP or MLD snooping
	
	[See Understanding Multichassis Link Aggregation Groups.]

Layer 2 VPN	• Support for VPLS. The router supports a single VLAN for each virtual switch routing instance type. Junos OS Evolved does not support the `family vpls` option. To configure VPLS, configure the `instance-type virtual-switch` statement at the [`edit routing-instances` *`routing-instance-name`*] hierarchy level. If you configure normalized VLANs, either by not configuring VLAN IDs or by including the `vlan-id none` statement, then you must include the `service-type single` statement at the [`edit routing-instances` *`routing-instance-name`* `protocol vpls`] hierarchy level. [See Introduction to Configuring VPLS.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

	• 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).
	
	[See control-word , Configuring Entropy Labels, and FAT Flow Labels Overview.]
	
	• Support for redundant pseudowires for virtual private LAN service (VPLS). The router supports VPLS with LDP hot-standby, cold-standby model, and without BFD or CFM trigger.
	
	[See Redundant Pseudowires for Layer 2 Circuits and VPLS.]
	
	• IRB support for VPLS.
	
	[See Configuring VPLS and Integrated Routing and Bridging.]
	
	• Layer 2 VPN and L2 circuit support:
	
	  • L2 circuit—Targeted LDP signaling pseudowires and interoperability between different types of supported attachment circuit 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.]
	
	• Flow-aware transport for pseudowires (FAT) label and entropy label support for Layer 2 circuit and Layer 2 VPN.
	
	[See Configuring Entropy Labels, and FAT Flow Labels Overview.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

Layer 3 features	• Support for the following Layer 3 features:
	  • IP forwarding and exception packet handling
	  • IEEE 802.1Q (VLAN trunk) on IRB interfaces
	  • Address Resolution Protocol (ARP), neighbor discovery, unicast reverse-path forwarding, and ECMP
	  • LPM and fragmentation handling, ICMP redirect handling, VLAN tagging modes, neighbor solicitation, and Interface-based routing
	  • Longest prefix match
	  • Exception packets handling
	  • VLAN tagging modes
	  • Integrated routing and bridging (IRB)
	  • IPv4 and IPv6
	The router also supports interior gateway protocols such as OSPF, IS-IS, RIP, and ECMP for IPv4 and IPv6. [See Configure ICMP Features, Enabling VLAN Tagging, Neighbor solicitation, Understanding Unicast RPF (Routers), OSPF Overview, IS-IS Overview, and RIP User Guide.]

Layer 3 VPN	Support for the following Layer 3 VPN features:
	NOTE: VT interface-based Layer 3 VPN is not supported. Layer 3 VPN ping is supported only with the `vrf-table-label` configuration.
	• IP-VPN services:
	  • Instance-type virtual routing and forwarding (VRF) and virtual-router
	  • All control plane configuration options

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
	• Per-prefix and per-table label signaling • Layer 3 VPN support with ECMP • BGP polices support for different Layer 3 VPN use cases (for example, full mesh VPN, hub-spoke VPN, management VPN, and leaking routes) • Layer 3 VPN with vrt-table-label mode • Layer 3 VPN with chained composite mode • Import or export of routes across local VRF and global VRF **NOTE**: Table next hop is not supported. • Inter-autonomous system (inter-AS) options A, B, and C **NOTE**: Inter-AS option B can be deployed in hierarchical network design within a single IGP AS. • PE to CE routing protocols—Static, eBGP, IS-IS, OSPF, and RIP • IPv6 Provider Edge (6PE)/IPv6 VPN routing over MPLS (6VPE) with PE-CE routing-static and PE-CE BGPv6 [See Layer 3 VPNs User Guide for Routing Devices.]
MACsec	Supports Media Access Control Security (MACsec). [See Understanding Media Access control Security (MACsec).]

Table 1: ACX7332 Feature Support *(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) and 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 includes 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: ACX7332 Feature Support *(Continued)*

Feature	Description

	• Support for MPLS LSP statistics and RSVP-TE auto-bandwidth features. Support includes:
	  • MPLS LSP statistics for the following LSP types:
	  • LDP-signaled LSPs
	  • RSVP-signaled LSPs
	  • Static LSPs
	  • Bypass LSPs
	  • Container LSPs
	  • RSVP-TE auto-bandwidth
	[See LSP Overview, LDP Overview, RSVP Overview, and Configuring Optimized Auto-bandwidth Adjustments for MPLS LSPs.]

Multicast	• Support for multicast snooping in a VPLS for the following protocols:
	  • IGMPv1, IGMPv2, and IGMPv3 snooping in VPLS
	  • MLDv1 and MLDv2 snooping in VPLS
	  • IGMP and MLD snooping in VPLS with integrated routing and bridging (IRB)
	  • Protocol Independent Multicast support over VPLS with IRB
	[See Multicast Snooping for VPLS.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

	• Support for Layer 2 multicast-related features, including IGMP and MLD snooping. You can configure IGMP snooping with IGMPv1, IGMPv2, and IGMPv3, which includes support for:
	  • IGMP snooping in bridge domains
	  • IGMP snooping with integrated routing and bridging (IRB) configured in bridge domains
	  • MLD snooping in bridge domains
	  • MLD snooping with IRB configured in bridge domains
	  [See IGMP Snooping Overview and Understanding MLD Snooping.]
	• Support for IPv4 multicast for Layer 3. You can configure IGMP snooping with IGMPv2 and IGMPv3, which includes support for the following:
	  • Anycast RP
	  • IGMP filter
	  • IGMP querier
	  • Protocol Independent Multicast source-specific multicast (PIM SSM)
	  • PIM sparse mode (PIM SM)
	  [See IGMP Snooping Overview.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
	• Support for BGP MVPN. BGP over MPLS MVPN (also known as "next generation," or "NG," MVPN) running on multipoint LDP provider tunnels, where BGP MVPN is the intra-AS and PIM-SM and multipoint LDP point-to-multipoint (P2MP) tunnels is the data plane. [See Multiprotocol BGP MVPNs Overview.] • Multicast with IGMP or MLD snooping within VLANs for EVPN-MPLS. [See Overview of Multicast Forwarding with IGMP or MLD Snooping in an EVPN-MPLS Environment.]
Network management and monitoring	• Support for port mirroring with analyzers and encapsulated remote Switch Port Analyzer (ERSPAN). [See Port Mirroring and Analyzers.] • Support for SNMP.

Operations, Administration, and Maintenance	• Support for OAM. You can configure connectivity fault management (CFM), BFD, and the 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).

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
	• Support for IEEE Standard 802.3ah and 802.1ag for OAM CFM up MEPs over EVPN. [See IEEE 802.3ah OAM Link-Fault Management Overview and IEEE 802.1ag OAM Connectivity Fault Management Overview.] • Support for CFM and performance monitoring (Y.1731) protocols over Ethernet interfaces for `bridge` and `inet` services. [See Ethernet OAM Connectivity Fault Management.] • Support for native Y.1731 operational state sensors to provide statistics such as frame loss ratio, frame delay, frame delay variation, and availability for Y.1731 performance monitoring.
Protection against DDoS attacks	• Support for control plane distributed denial of service (DDoS) protection. [See Control Plane Distributed Denial-of-Service (DDoS) Protection Overview.]

Routing protocols	• Layer 3 and routing protocols IPv4, IPv6, BGP, IS-IS and ARP streaming sensor support using gRPC services.
	
	• Support for unicast reverse path forwarding (unicast RPF):
	
	  • Support for loose and strict mode
	
	  • Support for IPv4 and IPv6
	
	[See Understanding Unicast RPF (Routers).]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

	• Support for BGP flow specification (BGP flowspec).
	  • The following match conditions are not supported:
	  • Fragment for IPv6
	  • Packet length
	  • Port
	  • Source and 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 configuring interface groups in BGP flowspec filters.
	  [See Understanding BGP Flow Routes for Traffic Filtering and Configuring BGP Flow Specification Action Redirect to IP to Filter DDoS Traffic.]
	• BGP PIC edge support for `inet` and MPLS VPNs. The following features are not supported:
	  • Session-based repair
	  • BGP PIC over LDP over RSVP tunnel
	  • BGP PIC over SR-MPLS

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
	• 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.]
	• Support for entropy label for LDP, RSVP, L3VPN, and BGP-LU. [See Entropy label support for BGP Labeled Unicast (BGP-LU) and Configuring Entropy Labels.] • Support for BGP transport address family or BGP Classful Transport (BGP-CT) includes: • Service mapping over colored transport tunnels (RSVP, IS-IS flexible algorithm) to transport classes and map service routes over an intended transport class. The transport tunnels can span multiple domains (ASs or IGP areas). • Network slicing and interoperability between network domains. • IPv6 and segment routing–traffic engineered (SR-TE) color-only support. • IPv6 and BGP service routes with a color-only mapping community. • Enhanced transport-class configuration to provide precise resolution. [See use-transport-class.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description

Services Applications	• RFC 2544-based benchmarking tests. Support for Layer 2 reflection (bridge, L2CKT, L2VPN, EVPN-VPWS, EVPN-FXC, EVPN-MPLS, and VPLS), with family `ccc` or family `ethernet-switching` and for Layer 3 reflection (IPv4, L3VPN) with family `inet`. RFC 2544 tests are performed to measure and demonstrate the service-level agreement (SLA) parameters before activation of the service. The tests measure throughput, latency, frame loss rate, and back-to-back frames.
	
	[See RFC 2544-Based Benchmarking Tests for ACX Routers Overview.]
	
	• 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. TWAMP is often used to check compliance with service-level agreements. The support for this service is limited to the following features:
	
	  • IPv4 and IPv6 source and target addresses for clients, control connections, 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 software (the Routing Engine or the Packet Forwarding Engine) or the hardware
	
	  • Error reporting through system log messages only
	
	  • Unauthenticated mode only
	
	[See Understand Two-Way Active Measurement Protocol.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
	• Support for sFlow monitoring (ingress). [See sFlow Monitoring Technology and Understanding How to Use sFlow Technology for Network Monitoring.] • Inline active flow monitoring support for IPFIX and v9 export formats. We support ingress and egress sampling of IPv4 and IPv6 traffic on aggregated Ethernet and IRB interfaces and interfaces mapped to non-default VRFs, for both the IPFIX and version 9 export formats. You can configure up to four IPv4 collectors for inline active flow monitoring. See Understand Inline Active Flow Monitoring.

Source Packet Routing in Networking (SPRING) or segment routing	• Support for the following segment routing features:
	
	  • Segment routing global block (SRGB) for OSPF, IS-IS, and fast reroute.
	
	  • Metro Ethernet services over segment routing infrastructure
	
	  • Segment routing services: L3VPN, IPv6 VPN Provider Edge (6VPE) , IPv6 Provider Edge (6PE), L2VPN, 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

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
	• Unnumbered interfaces support for segment routing with OSPF • Support for IPv6 L3VPN over IPv6 SR-TE and IPv6 underlay • Support for flexible algorithm in OSPF and IS-IS for segment routing traffic • Interoperability of segment routing with LDP • SPRING support for SR-TE • Support for BGP link-state distribution with SPRING extensions [See Understanding Topology-Independent Loop-Free Alternate with Segment Routing for IS-IS, Understanding Source Packet Routing in Networking (SPRING), Understanding Adjacency Segments, Anycast Segments, and Configurable SRGB in SPRING, Configure Unnumbered Interfaces, Understanding Static Segment Routing LSP in MPLS Networks, Link-State Distribution Using BGP Overview, Understanding OSPF Flexible Algorithm for Segment RoutingHow to Configure Flexible Algorithms in IS-IS for Segment Routing Traffic Engineering, and Mapping Client and Server for Segment Routing to LDP Interoperability.] • Support for SRv6 network programming in BGP and IS-IS. [See Understanding SRv6 Network Programming and Layer 3 Services over SRv6 in BGP and How to Enable SRv6 Network Programming in IS-IS Networks.] • Support for OAM ping and traceroute for Segment Routing for IPv6 (SRv6) network programming. [See ITU-T Y.1731 Ethernet Service OAM Overview and How to Enable SRv6 Network Programming in IS-IS Networks.] • Support for SRv6 flexible algorithms in traffic engineering database (TED) and BGP Link State (BGP-LS)

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
	[See How to Configure Flexible Algorithms in IS-IS for Segment Routing Traffic Engineering and BGP Link-State Extensions for Source Packet Routing in Networking (SPRING).] • SRv6 support for static SR-TE policy. [See Understanding SR-TE Policy for SRv6 Tunnel.] • Support for SRv6 micro-SIDs in IS-IS transport. You can compress multiple SRv6 addresses into a single IPv6 address (micro-SID). For use cases that need to include more than six SRv6 SIDs, micro-SIDs can help in compressing multiple IPv6 addresses. [See How to Enable SRv6 Network Programming in IS-IS Networks.]
Software installation and upgrade	• Support for secure-boot implementation based on the UEFI 2.4 standard. [See Software Installation and Upgrade Guide.] • Zero-touch provisioning (ZTP) support for WAN interfaces and DHCPv6 options. [See Zero Touch Provisioning.] • Secure Zero Touch Provisioning. [See Secure Zero Touch Provisioning.]
System management	• Support for an alternate partition for device recovery. You can use an alternate partition called **/altconfig** to recover the device when the **/config** partition gets corrupted. In certain scenarios, the **/config** partition (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** partition is corrupted. This is a boot-time feature and is enabled by default.

Table 1: ACX7332 Feature Support *(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.
	
	The ACX7332 router 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
	
	[See enable-extended-ql-tlv, Ethernet Synchronization Message Channel Overview, and synchronization.]
	
	• Support for frequency synchronization using the Synchronous Ethernet protocol in accordance with the ITU-T G.8262 and G.8262.1 standards. [See Synchronous Ethernet Overview.]
	
	• Synchronous Ethernet over LAG with Ethernet Synchronization Message Channel (ESMC).
	
	[See Synchronous Ethernet and Ethernet Synchronization Message Channel (ESMC).]
	
	• SNMP MIB support for the Synchronous Ethernet timing feature.
	
	[See Configuring SNMP Trap Groups and Enterprise-Specific MIBs for Junos OS Evolved.]
	
	• Support for G.8275.1 telecom profile, Precision Time Protocol over Ethernet (PTPoE) encapsulation, and hybrid mode. [See Precision Time Protocol Overview and Understanding Hybrid Mode.]
	
	• PTP G.8275.1 support over Link Aggregation Group (LAG)
	
	[See G.8275.1 Telecom Profile.]

Table 1: ACX7332 Feature Support *(Continued)*

Feature	Description
Support for optics	• To view the hardware compatibility matrix for optical interfaces, transceivers, and DACs supported on the ACX7332 router, see the Hardware Compatibility Tool.

•

Authentication and Access Control

- **OpenSSH upgrade to version 9.4 (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we've upgraded the version of OpenSSH from 7.5 to 9.4. The following SSH changes are a result of this upgrade:

  - The preferred signing algorithm has changed from ECDSA to ED25519.
  - The `scp` command now uses Secure File Transfer Protocol (SFTP) for file transfers by default. If you prefer to use the legacy SCP protocol, include the `-O` option when running the `scp` command.
  - SSH protocol version 1 has been removed.

  [See Configure SSH Service for Remote Access to the Router or Switch.]

Class of Service

- **Support for HCoS configurable deep buffer (ACX7024, ACX7024X, ACX7100, ACX7332, ACX7348, and ACX7509)**—Starting in Junos OS Evolved Release 24.2R1, we support fine-grained buffer configuration for hierarchical class of service (HCoS) on ACX Series routers. You can configure both the guaranteed buffer and shared buffer for each queue.

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

- **Support for HCoS on aggregated Ethernet interface (ACX7024, ACX7024X, ACX7100, ACX7332, ACX7348, and ACX7509)**—Starting in Junos OS Evolved Release 24.2R1, you can use hierarchical class-of-service (HCoS) configuration on aggregated Ethernet (`ae-`) interfaces on ACX Series routers.

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

EVPN

- **Support for EVPN-VPWS over SRv6-TE and SRv6 with micro-SID (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)** —

Starting in Junos OS Evolved Release 24.2R1, we support the following Segment Routing for IPv6 (SRv6) underlay features with EVPN-VPWS on the ACX7000 family:

- SRv6-TE tunnels without fallback support—With SRv6-TE, you can assign traffic flows to different networking SRv6 tunnels based on a customer's traffic service requirements.

  [See Overview of VPWS with EVPN Signaling Mechanisms, Configuring EVPN VPWS over SRv6 with Traffic Engineering, and Configuring EVPN over Transport Class Tunnels.]

- SRv6 with micro-SIDs—With micro-SID, you can compress multiple Segment Routing for IPv6 (SRv6) addresses into a single IPv6 address (the micro-SID and reduce bandwidth overhead.

  [See Configuring Micro-SIDs in EVPN-VPWS.]

- **Support for EVPN-MPLS (ELAN and IRB) over colored and non-colored SR-TE (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)**—Starting in Junos OS Evolved Release 24.2R1, we support EVPN services with underlay as SR-TE Policy over colored and non-colored SRTE. To configure colored SR-TE, include the `preserve-nexthop-hierarchy` statement at the `[edit routing-options resolution]` hierarchy level.

  This feature also supports EVPN asymmetric IRB over SR-TE. If you use Layer 3 (L3) gateway functionality with EVPN, asymmetric IRB flow over SR-TE doesn't work in a single pass. Therefore, asymmetric IRB flow uses a recycle path. The recycle handling requires specifying a recycle port and bandwidth. Thus, traffic over EVPN asymmetric IRB over SR-TE is restricted to the available recycle bandwidth.

  To reserve the bandwidth for EVPN IRB asymmetric flow, use the following configuration under `recycle-bandwidth-profile` to allocate a bandwidth:

  ```
  user@host# set system packet-forwarding-options recycle-bandwidth-profiles profile-name evpn-irb evpn-irb
  ```

  You can set the value for the *evpn-irb* bandwidth in the range of 1 through 100.

  Use the following configuration to activate the recycle bandwidth configuration:

  ```
  user@host# set system packet-forwarding-options recycle-bandwidth profile profile-name
  ```

  Use the following command to check the existing bandwidth usage:

  ```
  user@host> show system packet-forwarding-options recycle-bandwidth-profile
  ```

  If you do not reserve a bandwidth for the EVPN IRB application, the EVPN IRB application shares bandwidth with other recycle applications.

The following scenarios are supported:

- EVPN-ELAN over non-colored SR-TE without preserve next-hop hierarchy
- EVPN-ELAN over non-colored SR-TE with preserve next-hop hierarchy
- EVPN-ELAN single homing over colored SR-TE with preserve next-hop hierarchy
- EVPN-ELAN A/A multihoming homing over colored SR-TE with preserve next-hop hierarchy
- EVPN-ELAN A/S multihoming homing over colored SR-TE with preserve next-hop hierarchy
- EVPN-ELAN IRB symmetric over colored SR-TE with preserve next-hop hierarchy
- EVPN-ELAN IRB asymmetric over colored SR-TE with preserve next-hop hierarchy
- EVPN-ELAN over static SR-TE tunnel
- EVPN-ELAN over dynamic (DTM) SR-TE tunnel
- EVPN ELAN over SR-TE LSP path redundancy
- EVPN ELAN over SR-TE LSP and IGP redundancy
- EVPN aliasing over SR-TE with SR-TE and IGP-level redundancy
- EVPN IRB asymmetric over aliasing with SR-TE and IGP-level redundancy
- BGP-LU over SR-TE (non-preserve next-hop hierarchy mode only)
- Flow label over SR-TE
- NSR support for EVPN over SR-TE (SH, MH, IRB)

Interfaces

- **Smart SFP transceivers to transport TDM line traffic (ACX7024 and ACX7024X)**—Starting in Junos OS Evolved Release 24.2R1, we support the following smart SFP transceivers on the ACX7024 and ACX7024X routers:
  - DS3 smartSFP (SFP-GE-TDM-DS3)
  - E1 smartSFP (SFP-GE-TDM-E1)
  - T1 smartSFP (SFP-GE-TDM-T1)
  - STM1 smart SFP (SFP-GE-TDM-STM1)
  - STM4 smart SFP (SFP-GE-TDM-STM4)
  - STM16 smart SFP+ (SFP-XGE-TDM-STM16)

Every pair of Smart transceivers implements a Time Division Multiplexing (TDM) Circuit Emulation Service where TDM lines are transported transparently across a packet-switched network (PSN).

You can use these transceivers to transport TDM lines traffic such as E1 or T1 or DS3 or STM-1/OC-3, STM-4/OC-12, or STM-16/OC-64 encapsulated into data packets across PSNs such as Ethernet, VLAN-based, or MPLS networks. At the receiver end, another Smart transceiver, paired with the first one and appropriately configured, re-assembles the packets into the original bit stream and delivers it on its TDM line interface.

[See tdm-options (Interfaces).]

Junos Telemetry Interface

- **Support for OpenConfig MAC address and MAC address and IP path sensor (ACX7024, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Junos OS Evolved Release 24.2R1 supports streaming telemetry data for MAC addresses and MAC addresses and IP paths from the forwarding database to a collector using the resource path (sensor) **/network-instances/network-instance/fdb/**. This feature is based on data models **openconfig-network-instance.yang** (version 1.2.0) and **openconfig-network-instance-l2.yang** (version 1.2.0).

  [See Junos YANG Data Model Explorer.]

- **OpenConfig configuration and sensor support for AFI-SAFI policies (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Junos OS Evolved Release 24.2R1 supports export and import policies for address family indicator (AFI) and subsequent address family identifier (SAFI). OpenConfig support is for IPv4 and IPv6 unicast address families. Junos CLI-configured policies have priority over those configured with OpenConfig. For example, if different policies are configured for the same neighbor, one through an OpenConfig configuration and the other through a Junos CLI configuration, the latter policy takes effect.

  We support these OpenConfig configurations:

  - **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi<IPV4/V6_UNICAST>/apply-policy/config/import-policy**
  - **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi<IPV4/V6_UNICAST>/apply-policy/config/export-policy**

  We support these state sensors:

  - **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi<IPV4/V6_UNICAST>/apply-policy/state/import-policy**
  - **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi<IPV4/V6_UNICAST>/apply-policy/state/export-policy**

[For configurations, see Mapping OpenConfig BGP Commands to Junos Configuration. For sensors, see Junos YANG Data Model Explorer.]

- **Support for native LLDP, DCBX, MVRP, and MAC rewrite sensors in genstate YANG data models (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Junos OS Evolved Release 24.2R1 supports subscribable YANG data models for operational state on Junos devices. The genstate YANG models expose a subset of `show` command data through the gNMI subscribe RPC. A gNMI telemetry collector can subscribe to the resource paths defined in the published models to query for specific state data. This feature provides genstate YANG data model support for Link Layer Discovery Protocol (LLDP), Data Center Bridging Capability Exchange (DCBX), Multiple VLAN Registration Protocol (MVRP), and Layer 2 protocol tunneling (L2PT) MAC rewrite.

  [See Junos Genstate YANG Data Models and gNMI Genstate Subscription.]

- **Configure an IP source address and routing instance for legacy gRPC dial-out connections (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Junos OS Evolved Release 24.2R1 supports configuring a source IP address and routing instance for remote procedure call (gRPC) service dial-out connections. In earlier releases that support legacy gRPC dial-out, the outgoing interface IP address is used as the source address without an option to configure a source IP address. This feature supports FLEX Deployments, providing the ability to send dial-out from the router's specified IP address or interface address (such as a `loopback0` address).

  Use the `routing-instance` statement at the `[edit services analytics export-profile` *`profile-name`*`]` hierarchy level and the `local-address` *`ipv4 or ipv6 address`* statement at the `[edit services analytics export-profile` *`profile-name`*`]` hierarchy level.

  [See Using gRPC Dial-Out for Secure Telemetry Collection, routing-instance, and local-address.]

Layer 2 VPN

- **Support for hierarchical VPLS mesh groups and hot-standby convergence (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)**—Starting in Junos OS Evolved Release 24.2R1, you can configure mesh groups in an hierarchical VPLS (H-VPLS) network. The router supports:

  - Up to 3 mesh-groups with no-local switching in a single VPLS routing instance.
  - A total maximum of 14 mesh-groups with either local switching or no-local switching per routing instance.

  To configure mesh groups on ACX Series routers:

  - Configure the `routing-instances` *`routing-instance-name`* `protocols vpls` statement on the routers in the mesh group in the routing instance.

- Include the `system packet-forwarding-options system-profile vpls-meshgroups` statement on the routers in the H-VPLS network. The packet forwarding engine (PFE) restarts upon the issue of this command.

When you enable `vpls-hot-standby-convergence`, the Junos device sends advertising messages with different labels on the active and standby pseudowire. The spoke device can then differentiate the return messages coming back from the active and standby pseudowire. To enable hot-standby convergence improvement, include the `set routing-options forwarding-table vpls-hotstandby-convergence` statement at the spoke devices.

[See mesh-group (Protocols VPLS), packet-forwarding-options and Configure Hot-Standby Pseudowire Redundancy in H-VPLS.]

MPLS

- **Support for LDP dual transport over IPv4 and IPv6 sessions with NSR configuration (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can configure the LDP dual transport mechanism to establish IPv4 and IPv6 sessions with NSR configurations. This configuration helps in forwarding IPv4 and IPv6 traffic and to support LDP IPv6 sessions in a routing instance.

  [See Carrier-of-Carrier VPNs, LDP Overview, and LDP Configuration.]

- **Distributed CSPF support for IPv6-based SR-TE (ACX7024 and PTX10001-36MR)**—Starting in Junos OS Evolved Release 24.2R1, we support distributed CSPF path computation and auto-translation of IPv6 addresses through SR-TE configuration. A path's destination address family determines the address family of the SIDs used for the path. Configuring IPv6 addresses through SR-TE results in auto-translation of IPv6 addresses to the associated SIDs. IPv6 hops are defined in compute segment-lists.

  Use the following CLI configurations to enable auto-translation of IPv6 addresses:

```
user@host# set protocols source-packet-routing segment-list name auto-translate
user@host# set protocols source-packet-routing segment-list name name ip-address IPv6-address
```

  Use the following CLI configurations to define IPv6 hops in compute segment-lists:

```
user@host# set protocols source-packet-routing compute-profile name compute-segment-list name
user@host# set protocols source-packet-routing segment-list name compute
user@host# set protocols source-packet-routing segment-list name name ip-address IPv6-address
```

Use the following CLI configurations to enable IPv6 path end points:

```
user@host# set protocols source-packet-routing compute-profile name …
user@host# set protocols source-packet-routing source-routing-path name to IPv6-address
user@host# set protocols source-packet-routing source-routing-path name primary name compute
compute-profile-name
```

NOTE: End points must be IPv6 router IDs. Other addresses can be router IDs or interface addresses.

The `show spring-traffic-engineering lsp` command has been enhanced to show the details of IPv6 addresses.

- **Support for MPLS-over-GRE through next hop-based dynamic tunnel (ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, ACX7024, and ACX7024X)**—Starting in Junos OS Evolved Release 24.2R1, you can configure next-hop-based MPLS-over-GRE tunnels along with firewall filter-based tunnel decapsulation. MPLS-over-GRE tunnels create a tunnel composite next hop, an indirect next hop, and a forwarding next hop to resolve a tunnel destination route.

  You can configure dynamic GRE next-hop-based tunnel by including the `gre next-hop-based-tunnel` statement at the `[edit routing-options dynamic-tunnels]` hierarchy.

  You can configure MPLS-over-GRE firewall filter-based decapsulation by including the `gre` statement at the `[edit firewall family` *`family-name`* `filter` *`filter-name`* `term` *`term-name`* `then decapsulate]` hierarchy level. Only decapsulate action is supported in the firewall filter rule. MPLS-over-GRE firewall filter-based decapsulation is supported for family inet and inet6.

  You can retrive encapsulation tunnel statistics by configuring specific interval using the `interval` statement at the `[edit routing-options dynamic-tunnels statistics]` hierarchy level.

  [See Configuring Next-Hop-Based Dynamic GRE Tunnels.]

Multicast

- **L3 multicast statistics support (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)**—In earlier Junos OS Evolved releases, we supported hit-bit to indicate the liveness of each multicast route. Starting in Junos OS Evolved Release 24.2R1, you can enable Layer 3 (L3) multicast statistics to track the total number of packets and bytes that hit a (S,G) multicast route. The routes can be a combination of IPv4 and IPv6 (S,G) routes. We support both any-source multicast (ASM) and source-specific multicast (SSM) routes. To enable multicast statistics use the `mcast stats-enable` statement at the `[edit system packet-forwarding-options]` hierarchy level.

[See mcast stats-enable.]

Network Management and Monitoring

- **Clear LLDP neighbors from an interface with the gRPC Network Operations Interface (gNOI) `Layer2` service (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can execute supported `Layer2` service remote procedure calls (RPCs) to perform the equivalent of the `clear lldp neighbors interface` *`interface-name`* command.

  [See gNOI Layer 2 Service.]

- **Support for the `genstate` YANG data models (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we publish subscribable YANG data models for operational state on Junos devices. The `genstate` YANG models expose a subset of `show` command data through the gRPC Network Management Interface (gNMI) `subscribe` RPC. A gNMI telemetry collector can subscribe to the resource paths defined in the published models to query for specific state data.

  [See Junos Genstate YANG Data Models and gNMI Genstate Subscription.]

- **Support for NETCONF Call Home (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, Junos devices support the NETCONF Call Home feature for establishing a NETCONF session over SSH. NETCONF Call Home enables the Junos device to initiate a secure connection to a NETCONF client. You can use NETCONF Call Home when the NETCONF client cannot initiate a connection with the server. This situation can occur when a firewall or another security tool restricts management access to the server or implements Network Address Translation (NAT). NETCONF Call Home can also streamline the initial deployment of network devices by enabling a device to register with a management system when it is first powered on.

  [See NETCONF Call Home.]

Precision Time Protocol (PTP)

- **Support for SyncE MIB and PTP MIB (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, and ACX7348)**—Starting in Junos OS Evolved Release 24.2R1, the listed ACX Series devices support:

  - Defect and event management capabilities for timing features.

  - SNMP get, get-next, and walk management capabilities for timing features. These capabilities are enabled through the Synchronous Ethernet MIB (SyncE MIB) and Precision Time Protocol MIB (PTP MIB) timing objects.

[See Timing Defects and Event Management on Routing Platforms and SNMP MIB for Timing on Routing Platforms.]

- **Support for frequency and phase offset relaxation (ACX7100-32C and ACX7100-48L)**—Starting in Junos OS Evolved Release 24.2R1, you can relax the frequency and phase offsets required for a PTP lock on the listed ACX Series devices. To configure, use the `frequency-lock-threshold` and `phase-adjust-threshold` options of the `ptp` statement. You can also relax the maximum phase offset to adjust in a phase-aligned state by configuring the `phase-adjust-threshold` statement in the PTP configuration.

  [See ptp.]

- **Support for clearing PTP stream statistics (ACX7024, ACX7100-32C, ACX7100-48L, ACX7332, and ACX7348)**—Starting in Junos OS Evolved Release 24.2R1, you can clear the stream statistics for primary, client and stateful interfaces on the listed ACX Series devices. To clear the stream statistics, use the newly introduced `clear ptp statistics stream` command.

  [See clear ptp statistics stream.]

- **Automatic client support using subnet mask (ACX7100-32C and ACX7100-48L)**—Starting in Junos OS Evolved Release 24.2R1, the listed ACX Series devices support clients over subnet masks automatically over both IPv4 and IPv6.

  [See Clock Clients.]

- **Support for PTP G.8275.2 over LAG (ACX7100-32C, ACX7100-48L, ACX7024)**—Starting in Junos OS Release 24.2R1, the ACX7100-32C, ACX7100-48L, and ACX7024 routers support PTP G.8275.2 enhanced profile features compliant with the International Telecommunication Union Telecommunication Standardization (ITU-T) G.8273.4 standards. The following key features are supported:

  - Support for ordinary clocks and boundary clocks.
  - Support for the alternate best master clock algorithm.
  - Support for full domain and packet-rate ranges.
  - Support for primary and secondary asymmetry values.
  - Support for manual mode (no unicast negotiation) and mixed mode.
  - Support for primary(active) and secondary link configuration.

  [See PTP Profiles.]

Routing Protocols

- **Support for OSPFv2 HMAC-SHA-2 keychain authentication (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004,**

PTX10008, and PTX10016)—Starting in Junos OS Evolved Release 24.2R1, you can enable OSPFv2 keychain module with HMAC-SHA2 (OSPFv2 HMAC-SHA2) authentication to authenticate packets reaching or originating from an OSPF interface. HMAC SHA2 algorithms include HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 as defined in RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*. We support these algorithms along with HMAC-SHA2-224. This feature ensures smooth transition from one key to another for OSPFv2 with enhanced security. We also support HMAC-SHA1 and HMAC-SHA2 authentication for virtual and sham links.

To enable OSPFv2 HMAC-SHA2 authentication, configure the `keychain` *`keychain-name`* configuration statement at the `[edit protocols ospf area` *`area-id`* `interface` *`interface-name`* `authentication]` hierarchy level and the `algorithm (hmac-sha2-224 | hmac-sha2-256 | hmac-sha2-384 | hmac-sha2-512)` option at the `[edit security authentication-key-chains key-chain` *`key-chain-name`*`]` hierarchy level.

To enable keychains authentication support for OSPFv2 virtual links, configure the `keychain` *`keychain-name`* configuration statement at the `[edit protocols ospf area` *`area-id`* `virtual-link` *`neighbor-id router-id`* `transit-area area-idauthentication]` hierarchy level.

To enable keychains authentication support for OSPFv2 sham links, configure the `keychain` *`keychain-name`* configuration statement at the `[edit protocols ospf area` *`area-id`* `virtual-link` *`neighbor-id router-id`* `transit-area area-idauthentication]` hierarchy level.

[See Understanding OSPFv2 Authentication .]

- **Support for dying-gasp PDU (ACX7024 and ACX7024X)**—Starting in Junos Evolved OS 24.2R1, you can enable the dying-gasp functionality.

  Dying gasp is a Operation, Administration, and Maintenance (OAM) link fault management (LFM) protocol data unit (PDU) sent by the local peer to remote peer equipment in the event of a power failure. ACX Series devices support remote fault detection (RFD), which is one of the features of OAM LFM. RFD discovers power failures and sends dying-gasp PDUs to the remote peer. Sending dying-gasp PDU allows the OS to gracefully shut down the link and helps in isolating the fault.

  The dying-gasp functionality is disabled by default. To enable it, use the `set system dgasp-int` CLI command.

  [See **Enabling Dying Gasp Functionality**.]

- **Support for SR TI-LFA paths for IS-IS and OSPF (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)**—Starting in Junos OS Evolved Release 24.2R1, you can configure a point of local repair (PLR) to create a topology-independent loop-free alternate (TI-LFA) backup path for prefix segment identifiers (prefix SIDs) derived from LDP mapping server advertisements. In a network configured with segment routing, IGP uses the LDP mapping server advertisements to derive prefix SIDs. Currently, we don't support LDP mapping server advertisements for IPv6.

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

- **Support for SRLG link constraint in FAD and delay normalization (ACX Series and PTX Series)**—Starting in Junos OS Evolved Release 24.2R1, we support Flexible Algorithm Definition (FAD) defined constraints related to admin-groups and shared risk link group (SRLG) as defined in RFC 9350, *IGP Flexible Algorithm*. We also support delay normalization on the listed platforms. During Flexible Algorithm (flex algo) computation, when the measured latency values are not equal and the difference is insignificant, IS-IS advertises this slightly higher latency value as a metric. IS-IS uses this normalized latency delay value instead of the measured delay value.

  To configure flex-algo application-specific SRLG values, include the `application-specific` statement at the `[edit protocols isis interface interface-name level level]` hierarchy level.

  To exclude the SRLG constraint from an FAD, use the `exclude-srlg` statement at the `[edit routing-options flex-algorithm name definition]` hierarchy level.

  [See delay-measurementlevel, and definition.]

- **HMAC authentication with hash functions for IS-IS (ACX7024, ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we extend support to IS-IS keychain with the following hash functions:

  - HMAC-SHA2-224
  - HMAC-SHA2-256
  - HMAC-SHA2-384
  - HMAC-SHA2-512

  Currently, IS-IS supports inline authentication using simple password, keyed MD5, and HMAC-SHA1 algorithms with a common keychain. Note that it's important to have the system time synchronized on all nodes when a keychain is active on an IS-IS session.

  [See Understanding Hitless Authentication Key Rollover for IS-IS.]

- **BGP link bandwidth community (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016, and PTX12008)**—Starting in Junos OS Evolved Release 24.2R1, BGP can communicate link speeds to remote peers, enabling better optimization of traffic distribution for load balancing. A BGP group can send the *link-bandwidth* non-transitive extended community over an EBGP session for originated or received and readvertised link-bandwidth extended communities.

  To configure the non-transitive link bandwidth extended community, include the `bandwidth-non-transitive:value` in the export policy at the `[edit policy-options community name members community-ids]` hierarchy level.

  To enable the device to automatically detect and attach the link-bandwidth community on a route at import, include the `auto-sense` statement at the `[edit protocols bgp group link-bandwidth]` hierarchy level.

This feature facilitates the integration of devices with different transmission speeds within the network, enabling efficient traffic distribution based on link speed.

[See auto-sense, and group (Protocols BGP).]

- **Support for configuring multiple independent IGP instances of OSPFv2 (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can configure and run multiple independent IGP instances of OSPFv2 simultaneously on a router as defined in RFC 6549, *OSPFv2 Multi-Instance Extensions*.

  With this feature:

  - You can use multiple IGP instances of OSPFv2 to redistribute routes among independent OSPFv2 domains on a single router.
  - You can construct flexible OSPFv2 hierarchies across independent IGP domains.
  - You can achieve a more scalabale OSPFv2 deployment.

  To enable multiple IGP instances of OSPFv2 routing on the routing device, configure `ospf-instance` *`igp-instance-name`* at the `[edit protocols ospf]` hierarchy level.

  > **NOTE**: Junos OS Evolved does not support configuring the same logical interface with multiple IGP instances of OSPFv2.

  [See Multiple Independent IGP Instances of OSPFv2 Overview.]

Securing GTP and SCTP Traffic

- **Configurable TEID inclusion in GTP (ACX7100-32C, ACX7100-48L, ACX7509, and ACX7024)**– Starting in Junos OS Evolved Release 24.2R1 support for packet load balancing is based on the tunnel endpoint ID (TEID) of the GPRS Tunneling Protocol (GTP).

  > **NOTE**: There is no switch to enable or disable this functionality.

  Provided that ECMP is enabled on the device with multiple routes, the device automatically detects the TEID in the GTP header and includes it in the load-balancing hash.

  [See Understanding Per-Packet Load Balancing.]

Serviceability

- **Support for enhanced request support information (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we've deprecated the CLI option `brief` from the `request support information` command and introduced the following CLI options to the existing `request support information` command:

  - `archive`
  - `with-logs`
  - `with-components`
  - `with-options`.

  [See request support information.]

Services Applications

- **FTIs with support for UDP encapsulation (ACX7024, ACX7024X, ACX7100-48L, ACX7100-32C, ACX7332, ACX7348, and ACX7509)**—Starting in Junos OS Evolved Release 24.2R1, you can configure flexible tunnel interfaces (FTIs) that provide support for static UDP tunnels only.

  With the UDP tunnels-over-FTI feature, you can benefit from better traffic distribution over ECMP, which is achieved by the UDP source port derived from the hash value of the inner payload. The other benefits of this feature include shortened interface hop counts, smooth IGP domain separation, and reduced operational complexity.

  [See Flexible Tunnel Interfaces Overview.]

- **MPLS support for FTI tunnels (ACX7024X, ACX7100-48L, ACX71000-32C, ACX7024, ACX7509, ACX7348 and ACX7332)**—Starting In Junos OS Evolved Release 24.2R1, you can configure MPLS protocols over flexible tunnel interfaces (FTIs), thereby transporting MPLS packets over IP networks that do not support MPLS. GRE and UDP tunnels support MPLS protocol for both IPv4 and IPv6 traffic. You can configure encapsulation and de-encapsulation for the GRE and UDP tunnels.

  To allow the MPLS traffic on the UDP tunnels, include the `mpls` *`port-number`* statement at the `[edit forwarding-options tunnels udp port-profile` *`profile-name`*`]` hierarchy level. To allow the MPLS traffic on the GRE tunnels, include the `mpls` statement at the `[edit interfaces` *`fti0`* `unit` *`unit`* `family]` hierarchy.

  [See Flexible Tunnel Interfaces Overview.]

- **Support for layer 3 VPN service over logical tunnel interface (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)**—Starting in Junos OS Evolved Release 24.2R1, we support layer 3 VPN service over logical tunnel interfaces. The feature includes support for :

  - VRF over logical tunnel interface

- Stitching of layer 3 VPN and layer 2 services through logical tunnel interface

[See mac-vrf.]

- **Support for logical tunnel physical interface configuration (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)**—Starting with Junos Evolved OS Release 24.2R1, ACX7000 routers support logical tunnel physical interface configuration and Layer 2 services over logical tunnel interfaces.

  [See Guidelines for Configuring Logical Tunnels on ACX Series Routers.]

- **Support for configuring GRE tunnel encapsulation and de-encapsulation on flexible tunnel interfaces (ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, ACX7024, and ACX7024X)**—Starting in Junos OS Evolved Release 24.2R1, you can configure encapsulation by using the `tunnel encapsulation gre source` *address* `destination` *address* command at the `[edit interfaces fti unit` *unit*`]` hierarchy level.

  - If you add the `tunnel-termination` statement at the `[edit interfaces fti unit` *unit* `tunnel encapsulation gre]`, it makes the tunnel a de-encapsulation-only tunnel and disables encapsulation.

    The tunnel-termination only mode is not supported.

  - You must specify both the source and destination address if you do not configure the `tunnel-termination`.

  - You cannot configure a variable prefix mask on the source address.

  - You cannot configure `key` value.

  [See encapsulation and tunnel-termination.]

Software Installation and Upgrade

- **Base OS update (ACX Series and PTX Series)**—Starting in Junos OS Evolved Release 24.2R1, Junos OS Evolved uses the Wind River Linux LTS 22 base OS. This upgrade provides improved security and better performance. In earlier releases, Junos OS Evolved used the Wind River Linux LTS 19 base OS.

- **Migrate to GPT disk partitioning (ACX Series and PTX Series)**—Starting in Junos OS Evolved Release 24.2R1, we support migrating to GUID Partition Table (GPT) disk partitioning. GPT is the native disk partitioning scheme used by UEFI BIOSes. GPT is similar to the Master Boot Record (MBR) disk partitioning scheme used by traditional BIOSes. All Junos OS Evolved platforms support GPT natively. However, we default to MBR disk partitioning because Junos OS Evolved was originally ported to systems that used traditional BIOSes.

  GPT has several advantages over MBR:

  - Support for much larger disks

- Unique partition ID support by using GUIDs
- Human-readable partition names
- Backup copies

When you install a release that supports GPT disk partitioning, you can:

- For new installations, change the default partition scheme for both the primary and secondary disks to GPT immediately (for example, scratch installations to empty disks).
- For existing installations, migrate to GPT disk partitioning for both the primary and secondary disks after a reboot of the system.

[See Software Installation and Upgrade Overview (Junos OS Evolved).]

- **Support for SZTP (ACX7100-32C, ACX7100-48L, PTX10004, PTX10016, and PTX10001-36MR)**—Starting in Junos OS Evolved Release 24.2R1, you can use RFC-8572-based secure zero-touch provisioning (SZTP) to bootstrap your remotely located network devices that are in a factory-default state. SZTP enables mutual authentication between the bootstrap server and the network device before the remote network device is accessed for initiating ZTP.

  To enable mutual authentication, you need a unique digital voucher, which is generated based on the DevID (digital device ID or cryptographic digital identity) of the network device. The DevID is embedded inside the Trusted Platform Module (TPM) 2.0 chip ONLY on ACX7100-48L-*xxx*-K, ACX7100-32C-*xxx*-K, and PTX10001-36MR-K network devices. Juniper Networks issues a digital voucher to customers for each eligible network device.

  [See Secure Zero Touch Provisioning.]

-

- **Support for executing a pre-upgrade script with SZTP (ACX7024, ACX7100-32C, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can execute a pre-upgrade script to download signing keys or certificates for your third-party applications before provisioning your device. You can use the `pre-upgrade-script` XML tag to provide a pre-upgrade script as part of your onboarding information for SZTP.

  [See Secure Zero Touch Provisioning.]

- **Support for executing a pre-upgrade script with ZTP (ACX7024, ACX7100-32C, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can execute a pre-upgrade script to download signing keys or certificates for your third-party applications before provisioning your device. You can also use a pre-upgrade script to specify the management and WAN interface names and the speed of the WAN interfaces for ZTP. ZTP uses this information to avoid cycling through the unnecessary speed groups where the interface does not reside.

You can use DHCP option 43 suboption 9 for DHCPv4 and DHCP option 17 suboption 9 for DHCPv6 to specify the name of your pre-upgrade script as part of the bootstrap information. You can also toggle the behavior for DHCPv4 option 43 suboption 5 to specify either the IP address of the FTP server or the HTTP port.

[See Zero Touch Provisioning.]

- **Support for HTTP and HTTPS authentication on ZTP (ACX7024, ACX7100-32C, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can enable basic HTTP and HTTPS authentication for IPv4 and IPv6.

  To enable basic HTTP and HTTPS authentication for IPv4, use DHCP option 43 suboption 3. IPv6 ignores this option.

  For IPv6, provide the authentication parameters through the boot file URL and the URLs for the image, configuration, and alternate image. The precedence is the URL for the image, followed by the configuration, and then the alternate image. After that, the boot file URL is used. For authentication, the transfer type needs to be either HTTP or HTTPS.

  [See Zero Touch Provisioning.]

- **Support for HTTP and HTTPS proxy server on ZTP (ACX7024, ACX7100-32C, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can now configure an HTTP or HTTPS proxy server for ZTP.

  To specify an HTTP or HTTPS proxy server for IPv4, use DHCP option 43 suboption 8.

  To specify an HTTP or HTTPS proxy server for IPv6, use DHCP option 17 suboption 8.

  [See Zero Touch Provisioning.]

VLANs

- **`inner-list` option in the `vlan-tags` configuration statement (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)**—In Junos OS Evolved Release 24.2R1, we've added the `inner-list` option to the `vlan-tags` configuration statement. You can use the `inner-list` option to provide a list of VLAN identifiers.

  [See vlan-tags.]

Additional Features

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

- **EVPN VPWS service over SRv6** (ACX7024X and ACX7332)

  [See Configuring EVPN-VPWS over SRv6.]

- **Firewall filter support for ARP policer** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)

  [See ARP Policer Overview.]

- **Logical tunnel (lt-) interface support for EVPN E-LAN** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)

  [See Overview of VLAN Services for EVPN.]

- **Logical tunnel (lt-) interface support for EVPN-VPWS** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)

  [See Overview of VPWS with EVPN Signaling Mechanisms.]

- **NG-MVPN support** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, and ACX7509):

  - RSVP-TE P2MP link protection with a non-guaranteed convergence time of 50 ms
  - Segmented interarea P2MP LSPs

  [See Configuring Link Protection for Point-to-Multipoint LSPs and Segmented Inter-Area Point-to-Multipoint Label-Switched Paths Overview.]

- **NG-MVPN inter-AS support with RSVP-TE P2MP tunnels** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509):

  - Option-A
  - Option-B
  - Option-C

  [See Configuring Next Generation Layer 3 VPNs Options A, B, and C]

- **Paragon Active Assurance test agent** (ACX7024X). You can install a Paragon Active Assurance test agent on your router to monitor network quality, availability, and performance.

  [See Install the Paragon Active Assurance Test Agent.]

- **RFC 2544-based benchmarking tests with test generation and IEEE 802.3 bridging for Layer 2 Ethernet switching services** (ACX7024, ACX 7024X, ACX7100-32C, ACX7100-48L, ACX7332, and ACX7509)

  [See Layer 2 and Layer 3 RFC 2544-Based Benchmarking Test Overview.]

- **RFC 2544-based benchmarking tests with ingress reflection for Layer 2 Ethernet switching services** (ACX7024, ACX7100-32C, ACX7100-48L, and ACX7509)

  [See RFC 2544-Based Benchmarking Tests for ACX Routers Overview.]

- **sFlow egress support** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)

  [See sFlow Monitoring Technology.]

- **sFlow support for EVPN-VXLAN** (ACX7024, ACX7024X, ACX7100-32C, and ACX7100-48L)

  [See sFlow Monitoring Technology and EVPN-VXLAN Support for VXLAN Underlays on ACX Series Devices.]

- **Support for asynchronous notification for EVPN-VPWS** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)

  [See asynchronous-notification.]

- **Support for anycast gateways for Layer 3 VPN with MC-LAG** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)

  [See **Anycast Gateways**.]

- **Support for BGP-CT for EVPN-MPLS services** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)

  [See Configuring EVPN over Transport Class Tunnels and Color-Based Traffic Engineering Configuration.]

- **Support for BGP/MPLS MVPN** (ACX7332 and ACX7348). Starting in Junos OS Evolved 24.2R1, we support BGP/MPLS MVPN (also known as next-generation or NG MVPN) running on multipoint RSVP-Traffic Engineering (RSVP-TE) provider tunnels, where BGP multicast VPN (MVPN) is the intra-autonomous system and PIM source-specific multicast is the data plane.

  [See Multiprotocol BGP MVPNs Overview.]

- **Support for BGP-CT for EVPN-MPLS services** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)

  [See Configuring EVPN over Transport Class Tunnels and Color-Based Traffic Engineering Configuration.]

- **Support for BGP Prefix Independent Convergence (PIC) LU** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509). Starting in Junos OS Evolved Release 24.2R1, we support the following features with BGP PIC:

  - Session-based repair based on protocol convergence
  - BGP PIC over LDP over RSVP tunnel
  - BGP PIC with RSVP
  - BGP LU PIC support for L3VPN services (RSVP and LDP)

  - BGP PIC route resolution with `preserve-nexthop-hierarchy`
  - BGP LU PIC with preserve next-hop (RSVP and LDP)
  - BGP PIC over SR-MPLS
  - BGP PIC over IRB

  [See **BGP PIC Edge Using BGP Labeled Unicast Overview** and protect-core.]

- **Support for CFM maintenance association intermediate point (MIP)** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)

  [See OAM Connectivity Fault Management.]

- **Support for E-LINE services on EVPN VPWS FXC over SR TE** (ACX7024, ACX7024X, ACX7100-32C,ACX7100-48L, ACX7332, ACX7348, and ACX7509)We've extended support for E-LINE services on EVPN VPWS FXC over SR TE using MPLS on the ACX7000 family of routers.

  [See Overview of VPWS with EVPN Signaling Mechanisms and Configuring EVPN over Transport Class Tunnels.]

- **Support for EVPN E-LAN over SRv6 underlay** (ACX7024X and ACX7332)

  [See Configuring EVPN E-LAN over SRv6.]

- **Support for EVPN-ETREE** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)

  [See EVPN-ETREE Overview.]

- **Support for flex algo, FAPM leaking across IGP** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509). Starting in Junos OS Evolved Release 24.2R1, we support the following features:

  - IS-IS multi-instance
  - FAPM leaking across IS-IS multi-instance
  - FAPM leaking across OSPF and inter-area

  [See**How to Configure Multiple Independent IGP Instances of IS-IS**.]

- **Support for file system encryption with Trusted Platform Module (TPM 2.0)** (ACX7100-32C, ACX7100-48L, PTX10001-36MR, PTX10004, PTX10008, and PTX10016)

  [See Encryption with TPM.]

- **Support for Layer 2 VPN, Layer 2 circuit, and logical tunnel interfaces** (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)

  [See Layer 2 VPN, Layer 2 Circuits, and Logical Tunnel Interfaces.]

- **Support for Layer 3 over logical tunnel interfaces (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, and ACX7509)**—Starting in Junos OS Evolved Release 24.2R1, you can configure the families `inet` and `inet6`, and the following Layer 3 features over logical tunnel interfaces:

  - ARP
  - Exception packets
  - IGP and BGP
  - MTU handling
  - Neighbor Discovery Protocol (NDP)
  - Ping and traceroute
  - Unicast reverse-path forwarding (unicast RPF)
  - VLAN tagging
  - Virtual-router

- **Support for micro-SIDs in TI-LFA, microloop avoidance, flex algo, and IS-IS Multi Topology (IS-IS MT)** (ACX7024X, ACX7332, and ACX7348)

  [See **How to Enable SRv6 Network Programming in IS-IS Networks**.]

- **Support for monitoring MPLS LSP** (ACX7024, ACX7024X, ACX7100, ACX7332, ACX7348, ACX7509, PTX10004, PTX10008, PTX10016, PTX10001-36MR, and PTX10003, and the PTX10000-LC1202 line card)

  [See LSP Labels.]

- **Support for packet load balancing based on TEID of GTP** (ACX7024, ACX7100-32C, ACX7100-48L, and ACX7509)—There is no configuration to enable or disable this functionality. If ECMP is enabled on the device with multiple routes, the device detects the Tunnel Endpoint ID (TEID) in the GPRS Tunneling Protocol header and includes it the load-balancing hash automatically.

  [See Understanding Per-Packet Load Balancing.]

- **Support for VLAN-aware bundle service in EVPN-MPLS** (ACX7024X and ACX7332)

  [See Understanding VLAN-Aware Bundle and VLAN-Based Service for EVPN.]

- **Supported transceivers, optical interfaces, and DAC cables**—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.
- **Symmetric Type 2 EVPN-VXLAN to EVPN-VXLAN DCI stitching** (ACX7024, ACX7024X, ACX7100-32C, and ACX7100-48L)

  [See Symmetric Integrated Routing and Bridging with EVPN Type 2 Routes in EVPN-VXLAN Fabrics.]
- **Support for DevID** (ACX7100-32C and ACX7100-48L)—We introduce the digital cryptographic identity (also called device ID or DevID) feature embedded in TPM2.0 for ACX7100-32C and ACX7100-48L routers. DevID helps in mutual authentication of the network devices and thus enable secure zero touch provisioning (SZTP).

  [See SZTP Infrastructure Components.]

What's Changed

IN THIS SECTION

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

Authentication and Access Control

- **ChaCha20-Poly1305 algorithm deprecation for SSH cipher option**— The ChaCha20-Poly1305 authenticated encryption algorithm is deprecated for SSH cipher option. Configure aes-128-gcm and aes-256-gcm as the encryption algorithm for SSH Cipher option. [See ssh (System Services).]

EVPN

- **OISM SBD bit in EVPN Type 3 route multicast flags extended community**—In EVPN Type 3 Inclusive Multicast Ethernet Tag (IMET) route advertisements for interfaces associated with the supplemental bridge domain (SBD) in an EVPN optimized intersubnet multicast (OISM) network, we now set the SBD bit in the multicast flags extended community. We set this bit for interoperability with other vendors, and to comply with the IETF draft standard for OISM, draft-ietf-bess-evpn-irb-mcast. You can see this setting in the output from the `show route table bgp.evpn.0 ? extensive` command.

  [See CLI Commands to Verify the OISM Configuration.]

- **Group-based Policy (GBP) tag displayed with `show bridge mac-table` command**—On platforms that support VXLAN-GBP, the `show bridge mac-table` command now displays a GBP TAG output column that lists the GBP tag associated with the MAC address for a bridge domain or VLAN in a routing instance. Even if the device does not support or not using GBP itself, the output includes this information for GBP tags in packets received from remote EVPN-VXLAN peers.

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

- **Updates to syslog EVPN_DUPLICATE_MAC messages**—EVPN_DUPLICATE_MAC messages in the System log (syslog) now contain additional information to help identify the location of a duplicate MAC address in an EVPN network. These messages will include the following in addition to the duplicate MAC address:

  - The peer device, if the duplicate MAC address is from a remote VXLAN tunnel endpoint (VTEP).
  - The VLAN or virtual network identifier (VNI) value.
  - The source interface name for the corresponding local interface or multihoming Ethernet segment identifier (ESI).

  For example: `Feb 27 22:55:13 DEVICE_VTEP1_RE rpd39839: EVPN_DUPLICATE_MAC: MAC address move detected for 00:01:02:03:04:03 within instance=evpn-vxlan on VNI=100 from 10.255.1.4 to ge-0/0/1.0.`

  For more on supported syslog messages, see System Log ExplorerSystem Log Explorer.]

- **New commit check for MAC-VRF routing instances with the `encapsulate-inner-vlan` statement configured**— We introduced a new commit check that prevents you from configuring an IRB interface and the `encapsulate-inner-vlan` statement together in a MAC-VRF routing instance. Please correct or remove these configurations prior to upgrading to 23.2R2 or newer to avoid a configuration validation failure during the upgrade.

  [See encapsulate-inner-vlan.]

- **Optimized mesh group routes (ACX Series)**— `show route snooping` for inet.1 or inet6.1 table and `show route snooping table inet.1 | inet6.1` display only CE mesh group routes for platforms that support EVPN-MPLS or EVPN-VxLAN multicast. In earlier releases, other mesh groups like the VE mesh group were also displayed.

- **Limit on number of IP address associations per MAC address per bridge domain in EVPN MAC-IP database**—By default, devices can associate a maximum of 200 IP addresses with a single MAC address per bridge domain. We provide a new CLI statement to customize this limit, `mac-ip-limit` statement at the **edit protocols evpn** hierarchy level. In most use cases, you don?t need to change the default limit. If you want to change the default limit, we recommend that you don?t set this limit to more than 300 IP addresses per MAC address per bridge domain. Otherwise, you might see very high CPU usage on the device, which can degrade system performance.

  [See mac-ip-limit.]

Infrastructure

- **Option to disable path MTU discovery**—Path MTU discovery is enabled by default. To disable it for IPv4 traffic, you can configure the `no-path-mtu-discovery` statement at the [`edit system internet-options`] hierarchy level. To reenable it, use the `path-mtu-discovery` statement.

  [See Path MTU Discovery.]

Interfaces and Chassis

- ACX7509: In the CLI, using the command `request chassis feb slot slot-number offline`, if you make the primary FEB offline, a traffic loss warning message is displayed and the FEB offline request is rejected. If offline/restart is still intended for primary FEB, use the force option in addition to the command. WARNING message displayed in the CLI: **"warning: RCB and FEB work in the paired slot mode. FEB %s offline/restart will result in traffic loss and does not cause a switchover. Please re-try after initiating a mastership switchover using 'request chassis routing-engine master switch' CLI. If offline/restart is still intended, use 'force' option in addition to this CLI."**

Junos OS API and Scripting

- **<get-trace> RPC support removed (ACX Series and PTX Series)**—The `show trace application app-name` operational command and equivalent <get-trace> RPC both emit raw trace data. Because the <get-trace> RPC does not emit XML data, we've removed support for the <get-trace> RPC for XML clients.

Network Management and Monitoring

- **Change in use of RSA signatures with SHA-1 hash algorithm**—Starting in Junos OS Release 24.2R1, there is a behavioural change by OpenSSH 8.8/8.8p1. OpenSSH 8.8/8.8p1 disables the use of RSA signatures with SHA-1 hash algorithm by default. You can use RSA signatures with SHA-256 or SHA-512 hash algorithm.

Platform and Infrastructure

- Starting Junos Evolved Release, support for Network Time Protocol (NTP) over TLS (RFC 8915 compliant) for the ACX-series and PTX-series includes:
  - Support to configure local-certificate for server and certificate verification option for client.
  - Verification of x.509 certificates to establish a TLS channel between client and server. - TLS NTS-KE protocol support.
  - Support for NTS secured client-server NTP communication at server and client.
  - Support for new NTS options in commands `system ntp nts`, `system ntp server <server_name> nts remote-identity`, and `show ntp associations no-resolve` commands.

System Management

- **Additional `Upgrade` fields for the `show system applications detail` command (ACX Series and PTX Series)**—The `show system applications detail` command and corresponding RPC include additional `Upgrade` output fields. The fields provide information about notifications and actions related to various upgrade activities.

  [See show system applications (Junos OS Evolved).]

User Access and Authentication

- Starting in Junos OS Release and Junos OS Evolved Release, when you run the run `show lldp local-information interface <interface-name> | display xml` command, the output is displayed under the **lldp-local-info root** tag and in the **lldp-local-interface-info container** tag. When you run the run `show lldp local-information interface | display xml` command, the **lldp-tlv-filter** and **lldp-tlv-select** information are displayed under the **lldp-local-interface-info container** tag in the output.

- **Viewing files with the `file compare files` command requires users to have `maintenance` permission**—The `file compare files` command in Junos OS Evolved requires a user to have a login class with `maintenance` permission.

  [See Login Classes Overview.]

VPNs

- **Increase in revert-delay timer range**— The `revert-delay` timer range is increased to 600 seconds from 20 seconds.

- **Configure min-rate for IPMSI traffic explicitly**— In a source-based MoFRR scenario, you can set a min-rate threshold for IPMSI traffic explicitly by configuring `ipmsi-min-rate` under `set routing-instances protocols mvpn hot-root-standby min-rate`. If not configured, the existing `min-rate` will be applicable to both IPMSI and SPMSI traffic.

  [See min-rate.]

Known Limitations

IN THIS SECTION

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

- When the original flow egresses out through an aggregated Ethernet (AE) interface, the corresponding sampled sflow frame does not reflect the correct egress port number. This happens only when the flow is egresses out through an AE interface. For non-AE egress interface, this works fine and the sflow frame reflects the correct egress port.PR1647870
- While disabling and enabling all the lanes of 400G optics together, carrier transition count on random lanes might get incremented. There is no functional impact.PR1779602

Open Issues

IN THIS SECTION

Learn about open issues in this release for ACX Series routers

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

General Routing

- ACX7509: G.8275.1 FPC Dpll status is incorrectly shown in `timingd gencfg ptp centralized` command.PR1685675
- Suppose a user has disabled RE0 for primary role as follows: `set chassis redundancy routing-engine 0 disabled`. This prevents RE0 from becoming primary on system boot. Instead RE1 become primary. Under this scenario, an automatic fault-based switchover from RE1 to RE0 can still happen. The workaround is to disable automatic fault-based switchovers also as follows: `set chassis redundancy failover disable`.PR1713851
- We observe core file with rpd with BGP flowspec if secondary-independent-resolution is configured.PR1722715

- When ingress policer is configured, to drop ingress traffic, on an interface with upMep the CFM packets generated from the upMep are also dropped due to the policer. This leads to CFM session going down.PR1754938
- CFM sessions when scaled on ACX7000 Junos OS Evolved Series can get stuck in OK state on catastrophic events which can result in CCM timeouts at the same time. It can be recovered with CFMD process restart.PR1768708
- With DHCP trace options enabled in the regression scripts, core file is seen. Issue is random not seen always. This is enabled in script for debugging in production network this is not be enabled by default hence the issue is not seen. Its recommended to enable DHCP trace options only for debugging not otherwise.PR1771121
- Following error message is seen with the delete vlan event trigger when configured with multiple vlans with IRB and IGMP snooping/MLD snooping enabled. No functionality impact. **Error] compName = "BrcmPlusMcast", tpName = "Irb", msg = " fn = removeMemberFromL3FloodMcastGrp**. PR1771915
- Multihop BFD packets by default uses the network-control queue in Junos OS Evolved ACX Series. This setting remains same despite configuring the host-outbound-traffic to a different forwarding-class.PR1776127
- ACX7509 HA has dual feb and LT interface creation uses **feb slot id** as a keyword in CLI. As per the current design limitation, LT interface cannot be supported on ACX7509 HA platforms(in Junos OS Evolved Release 24.1R1). If user initiates `restart evo-pfemand` on primary Routing Engine or switchover on ACX7509 HA device, this results in complete traffic drop. PR1778116,PR1778137.
- On ACX7100-32C and ACX7100-48L, Precision Time Protocol (PTP) state remains **ACQUIRING** when the PTP is configured in Hybrid mode (Synchronous Ethernet (SyncE) + PTP) and PTP mode is committed at a time with PTP configuration. PR1783545
- ACX7509 :: For all sBFD sessions in scaled setup, to come up after link down event (sBFD FRR) , it is recommended to configure the lo0 interface with default local host ip. PR1788465
- During multiple RE (Routing Engine) switch-overs and router reboots, management port of one of the Routing Engines comes up with 100 MBPS speed instead of 1 GBPS speed. There is no functional or stability impact due to this issue. Router monitoring might face a mild performance issue due to this lower speed of management port.PR1789156
- L3VPN traffic over tunnels could drop with egress marking error when dynamic tunnels are configured, this is specific to all Junos Evolved ACX7000 variants. This can be checked by issuing `show pfe statistics error` output. PR1789481
- This is a day-1 issue. It exists on all ACX platforms where Juniper Networks servo runs. Once the asymmetry configured at the secondary port, the error propagated to the down stream eventually causes this performance issue of spike. PR1793926

- When multicast packets are transiton ACX7100 devices through VXLAN VTEP or core interface without multicast configurations, errors are seen. Suggested to use DDOS configurations provide with the workaround.

```
set system ddos-protection protocols ipmcast-miss aggregate bandwidth 100
set system ddos-protection protocols ipmcast-miss aggregate burst 1024
```

  PR1796501

- On all Junos OS Evolved platforms, when a layer 2 routing-instance is changed to layer 3 routing-instance or vice versa without changing the name of the routing-instance in a single commit, due to a rare timing issue, the rpd process can crash. During the rpd crash and restart, the routing protocols are impacted and traffic disruption is seen due to the loss of routing information. PR1802000

Routing Protocols

- Configuration of a global AS number is necessary when route target filter is enabled. Currently Junos OS CLI does not enforce configuring a global AS number and it has been the behavior for a long time. Many unexpected issues might be seen without a global AS number. It's been a recommended practice to configure a global AS number in the field.PR1783375

Resolved Issues

IN THIS SECTION

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.

General Routing

- G.8275.1- G.8273.2 1PPS cTE performance test might be marginally outside class-C intermittently on ACX7100-48L. PR1607381
- ACX Series reports **/psm/0/ hwdre/0/cm/0/ psm_mcu /psm0/psm_cml_cmd_fault** even though the PSM is in working order. PR1700839
- We might encounter jdhcpd core during initialization. The core in rare, and there is no service impact because of this core (as the process recovers immediately). PR1730717
- We observe continuous ssh errors on log messages (error: Could not load host key: **/etc/ssh/ssh_host_ec_p521_key**). PR1744354
- Port speed delete results in setting the it to the default speed. PR1748138
- Multiple Routing Engine switchover can cause IDEEPROM failure on FPC and PSM. PR1760978
- We observe spikes in 1pps performance during long run testing. PR1761078
- CRC errors observed with SFT-T (740-013111 & 740-027085) optics. PR1771671
- **/components/component/power-supply/** sensor leaves and values are not streamed in gNMI and the data is streamed through gRPC in latest primary 24.2 builds. PR1772435
- [Clocking Solution]:ACX7348:PTP and SyncE does not work properly after Routing Engine switch over. PR1775585
- RPD core file can be see when running Telemetry for protocols from top of tree and doing routing instance add delete operation. PR1778103
- Name resolution does not happen for `show arp` output. PR1778567
- After swtichover with MPLS FRR with VPLS configured, you observe that traffic to a few VPLS instances is dropped. PR1779466
- Junos OS Evolved: ACX7000 Series: Protocol specific DDoS configuration affects other protocols (CVE-2024-39531). PR1784343
- Policy based routing does not work as intended when it is configured with `next-ip` or `next-ip6` on all ACX Junos OS Evolved platforms except ACX7024. PR1784909
- STP bridge domain or ERPS protected domain configured on the IRB interface causes traffic to be dropped. PR1784990
- Route leaking between VRFs through the RIB group does not work as expected. PR1786295

- CFM configuration with multiple MEP under same maintenance-association causes evo-pfemand process crash and CFM session might not come up. PR1786395
- Autoneg configuration for 1G optical does not turn on upon inspecting PHY registers. PR1787154
- Syslog message with compName **= "RT", ddsType = "RouteCcc" tpName = "BrcmRtCcc", guid = "1026497426433" msg = " = serviceNhLookup Failed, op = Add**. PR1787689
- Interfaces with QSFP-100GBASE-LR4 optics might not come up after software upgrade or system reboot. PR1788848
- The evo-pfemand process crashes on Junos OS Evolved ACX Series platforms. PR1791199
- Junos ping inet command does not force IPv4 in Junos OS Evolved platforms. PR1792415
- Error messages are populated **getQosRewriteHwMapIdFromIflIndex** and interface ifd queue statistics traffic goes to the wrong queue. PR1793256
- PICD core file can be seen during FPC offline or online, HA switchover, and system restart. PR1793824
- FPCs are not recovered when system is rebooted right after Routing Engine switchover due to evo-pfemand crash. PR1797593
- Traffic drops observed in the L2Circuit or L2VPN scenario. PR1797839
- Traffic drops are seen on all Junos OS Evolved platforms. PR1798446
- Multiple create or delete of physical interface, Layer 3 and MACsec interfaces blocks MACsec traffic on Junos Evolved platforms. PR1800139
- [Junos OS Evolved] **Host 0 Disk 1 Labelled incorrectly** alarm is sometimes set and cleared in 5 seconds. PR1801436
- In platform ACX7509 after switchover, STP states re-converge even with NSB enabled. PR1801786
- CB goes into fault state after system Routing Engine power off or on using button press. PR1802508
- The MPLS tunnel traffic arriving at the ingress interface drops on ACX7000 platforms when storm control is enabled. PR1802525
- [ACX7000] With IPSEC-Ah configuration enabled, OSPF or OSPF3 session does not work. PR1803437
- Some timing features do not work as intended with PLL input and lock failure alarms on Junos OS Evolved platforms after Routing and Control Board jack in and switchover. PR1803481
- [ACX7000] Post instance renaming, VPLS MACs stops exchanging over MPLS core or LSI interface. PR1805586

- ACX7024 Timing : T-GM performance shows 1 second time offset. PR1808134
- L2ald-agent generates core file and IRB logical interface stays hardware-down after deletion of IRB (with virtual-gateway-address configuration) , reading same virtual-gateway-address as IRB address and move back to IRB with same virtual-gateway-address. PR1808779
- OSPFv3 neigborship forming issue on IRB when mld-snooping enabled on the BD where IRB hosted. PR1816540

EVPN

- Traffic drop in between EVPN hosts might be seen when `vlan-id none` is configured and any commit changes done under `protocols mpls`.PR1792566

Services Applications

- Junos OS Evolved Release 24.2 and later run a dnsmasq DNS caching service on tcp/udp port 53.PR1777424

User Interface and Configuration

- [Junos OS Evolved] Traceoptions log sometimes shows UTC timestamp, although non UTC time-zone is configured. PR1783888
- Configuration archival through FTP, doesn't work with presence of firewall filter on the loopback interface even when FTP ports are allowed. PR1798464

Junos OS Evolved Release Notes for PTX Series

IN THIS SECTION

These release notes accompany Junos OS Evolved Release 24.2R1 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 24.2R1, click the Group by Release link. You can collapse and expand the list as needed.

- PTX10001-36MR
- PTX10003
- PTX10004
- PTX10008
- PTX10016
- PTX10002-36QDD

The following sections highlight the key features in this release.

Hardware

- **New SKU (PTX10001-36MR-K)**—Starting in Junos OS Evolved Release 24.2R1, we introduce a new SKU, PTX10001-36MR-K, that has enhanced security feature.

  The PTX10001-36MR-K has all the hardware and software features of the PTX10001-36MR router along with a newly added Trusted Platform Module (TPM) 2.0 chipset. This chipset has an embedded DevID (digital device ID or cryptographic digital identity), which enables the Secure ZTP feature.

  The new PTX10001-36MR-K SKU can be distinguished by the label *PTX10001-36MR-K* on the device.

  When you use the CLI command *show chassis hardware* or *show version*, it displays the chassis or model name as *JNP10001-36MR-K [PTX10001-36MR-K]*.

- **New HVAC/HVDC Power Supply Unit (PSU) (PTX10004, and PTX10008)**—Starting in Junos OS Evolved Release 24.2R1, we introduce a new high-capacity HVAC/HVDC PSU (JNP10K-PWR-AC3H). The JNP10K-PWR-AC3H PSU is designed to support high voltage AC or high voltage DC systems in a 15 A or 20 A power mode. The PSU takes four single-phase HVAC (180-305 VAC) or HVDC (190 - 410VDC) inputs at either 20 A or 15 A and provides a DC output of 12.3V. The power supply contains five DIP switches on the faceplate to let you configure the power supply for high-power (20 A) or low-power (15 A) input mode.

[See PTX10004 Power System, and PTX10008 Power System.]

- **New DC Power Supply Unit (PSU) (PTX10004, and PTX10008)**—Starting in Junos OS Evolved Release 24.2R1, we introduce a new high-capacity DC PSU (JNP10K-PWR-DC3). The JNP10K-PWR-DC3 PSU is designed to support four power supplies in a single housing that accepts either 60 A or 80 A power from four input power feeds. The power supply contains five DIP switches on the faceplate to let you configure the power supply for high-power (80 A) or low-power (60 A) input mode.

  [See PTX10004 Power System, and PTX10008 Power System.]

- **Fan Tray and Fan Tray Controller (PTX10004, PTX10008)**—We introduce two new fan trays (JNP10004-FAN3 and JNP10008-FAN3) and two new fan try controllers (JNP10004-FAN-FTC3 and JNP10008-FAN-FTC3). The JNP10004-FAN3 and JNP10004-FAN-FTC3 are used in PTX10004 routers. The JNP10008-FAN3 and JNP10008-FAN-FTC3 are used in PTX10008 routers.

  Table 2: Fan Tray and Fan Tray Controller

Fan Tray	Fan Tray Controller	Router
JNP10004-FAN3	JNP10004-FAN-FTC3	PTX10004
JNP10008-FAN3	JNP10008-FAN-FTC3	PTX10008

  See PTX10004 Packet Transport Router Hardware Guide and PTX10008 Packet Transport Router Hardware Guide.

-

Authentication and Access Control

- **OpenSSH upgrade to version 9.4 (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we've upgraded the version of OpenSSH from 7.5 to 9.4. The following SSH changes are a result of this upgrade:

  - The preferred signing algorithm has changed from ECDSA to ED25519.
  - The `scp` command now uses Secure File Transfer Protocol (SFTP) for file transfers by default. If you prefer to use the legacy SCP protocol, include the `-O` option when running the `scp` command.
  - SSH protocol version 1 has been removed.

  [See Configure SSH Service for Remote Access to the Router or Switch.]

- **TACACS+ support for console access**— Starting in Junos OS Evolved Release 24.2R1 EVO, console support using local authentication is supported on PTX 10001-36MR, PTX 10003, and PTX10008 platforms regardless of whether local authentication is configured as per access authentication order.

  [See Authentication Order for RADIUS TACACS+, and Local Password].

Chassis

- **Support for Gen3 FT and FTC SKUs (PTX-Series)**—Starting in Junos OS Evolved Release 24.2R1, support is provided for the new fan trays (FT) (JNP10004 Fan-Tray Gen3 and JNP10008 Fan-Tray Gen3) and fan tray controllers (FTC) (JNP10004 Fan Controller Gen3 and JNP10008 Fan Controller Gen3) SKUs along with resiliency support for PTX10004 and PTX10008 devices.

- **Source Redundancy and Feed Redundancy support (PTX10004 and PTX10008)**—N+1 power redundancy is supported on PTX10004 and PTX10008 routers with the JNP10K-PWR-DC3 power supply modules (PSMs). You can enable either source redundancy or feed redundancy for the PSM.

  [See Power Redundancy for Third-Generation Power Supply Modules.]

- **Resiliency support (PTX10004 and PTX10008)**—We support resiliency for JNP10K-PWR-DC3 power supply modules (PSMs) on PTX10004 and PTX10008 devices. Resiliency enables the system to monitor component health, alert you of errors, and take appropriate action to restore normal operation based on error severity.

  [See Resiliency, thermal-health-check, and watchdog (PSM).]

- **Source Redundancy and Feed Redundancy support (PTX10004 and PTX10008)**—We provide N+1 power redundancy support on PTX10004 and PTX10008 routers with the JNP10K-PWR-AC3H power supply modules (PSMs). You can enable either source redundancy or feed redundancy for the PSM to ensure continuous power supply and enhance system reliability.

  [See Power Redundancy for Third-Generation Power Supply Modules.]

- **Resiliency support (PTX10004 and PTX10008)**—We provide resiliency feature support for JNP10K-PWR-AC3H power supply modules (PSMs) on PTX10004 and PTX10008 devices. Resiliency enables the system to monitor component health, alert you of errors, and take appropriate action to restore normal operation based on error severity.

  [See Resiliency, thermal-health-check, and watchdog (PSM).]

Class of Service

- **Support for per-logical interface queuing (PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, PTX10004, PTX10008, and PTX10016 routers support per-logical interface queuing, also known as per-unit scheduling. With per-unit scheduling enabled, you can configure up to:

- Six logical interfaces per physical port on the PTX10004 and PTX10008.
- Two logical interfaces per physical port on the PTX10016.

Each logical interface has its own set of eight queues. We also reserve a separate logical interface for port-level control protocols."

To enable per-logical interface queuing on an interface, set `per-unit-scheduler` at the `[edit interfaces interface-name]` hierarchy level.

[See **Configuring Queuing and Shaping on Logical Interfaces on PTX Series Routers**.]

High Availability

- **NSR switchover support with low hold timers (PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we support 8000 BGP sessions with variable hold timers as low as 3 seconds for nonstop active routing (NSR) switchovers. You can configure up to 400 highly sensitive BGP sessions with hold timers of 10 seconds or lower, with the remaining sessions configured at either the default hold time of 90 seconds or a sparse distribution of hold timers in the range of 30 seconds and higher.

  [See hold-time.]

- **Performance improvements for micro-BFD sessions with intervals lower than 50 ms (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you will see improved performance for micro-BFD sessions that are configured with timers under 50 ms in inline mode.

  [See Understanding Independent Micro BFD Sessions for LAG.]

- **Default support for configuring micro BFD with an interface IP address (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, micro BFD sessions support interface IP addresses by default.

  [See Understanding Independent Micro BFD Sessions for LAG.]

Interfaces

- **400G-ZR-M support enhancements (PTX10003)**—Starting in Junos OS Evolved Release 24.2R1, we support 400G-ZR-M optics enhancements on PTX10003 routers. The enhancements include application selection and configuration of target output power. You can view the advertised applications and can also switch between the applications.

  [See 400ZR and 400G OpenZR+.]

Junos Telemetry Interface

- **Support for OpenConfig MAC address and MAC address and IP path sensor (ACX7024, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Junos OS Evolved Release 24.2R1 supports streaming telemetry data for MAC addresses and MAC addresses and IP paths from the forwarding database to a collector using the resource path (sensor) **/network-instances/network-instance/fdb/**. This feature is based on data models **openconfig-network-instance.yang** (version 1.2.0) and **openconfig-network-instance-l2.yang** (version 1.2.0).

  [See Junos YANG Data Model Explorer.]

- **Alarms resource path enhanced with hardware component names (PTX10001-36MR, PTX10003, PTX10004, and PTX10008)**—Junos OS Evolved Release 24.2R1 enhances the **/system/alarms/alarm/state/** resource path to include hardware component names found in the OpenConfig data model **platform.yang**. For example, component names in the following format are also displayed at the same level in the alarms resource path for greater accuracy:

  - **/components/component[name= 'CHASSIS0:FPC0:PIC1:PORT2']/port**
  - **/components/component[name= 'CHASSIS0:RE0']/controller-card**
  - **/components/component[name= 'CHASSIS0:RE0:FPC1']/linecard**
  - **/system/alarms/alarm/state/resource CHASSIS0:RE0:FPC1**

  [See Junos YANG Data Model Explorer.]

- **Platform telemetry sensor support (PTX10004 and PTX10008)**—Junos OS Evolved Release 24.2R1 supports streaming, ON_CHANGE, INITIAL_SYNC, and TARGET_DEFINED subscription modes as well as zero-suppression. Sensors are supported for all PEMs and fans.

  These sensors are supported:

  - **/components/component/properties/property**
  - **/components/component/state/temperature**
  - **/components/component/state**
  - **/components/component/fan/state**
  - **/components/component/power-supply/state**

  [See Understanding OpenConfig and gRPC on Junos Telemetry Interface. For sensors, see Junos YANG Data Model Explorer.]

- **OpenConfig configuration and sensor support for AFI-SAFI policies (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Junos OS Evolved Release 24.2R1 supports export and

import policies for address family indicator (AFI) and subsequent address family identifier (SAFI). OpenConfig support is for IPv4 and IPv6 unicast address families. Junos CLI-configured policies have priority over those configured with OpenConfig. For example, if different policies are configured for the same neighbor, one through an OpenConfig configuration and the other through a Junos CLI configuration, the latter policy takes effect.

We support these OpenConfig configurations:

- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi<IPV4/V6_UNICAST>/apply-policy/config/import-policy**
- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi<IPV4/V6_UNICAST>/apply-policy/config/export-policy**

We support these state sensors:

- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi<IPV4/V6_UNICAST>/apply-policy/state/import-policy**
- **/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/afi-safis/afi-safi<IPV4/V6_UNICAST>/apply-policy/state/export-policy**

[For configurations, see Mapping OpenConfig BGP Commands to Junos Configuration. For sensors, see Junos YANG Data Model Explorer.]

- **Support for native physical interface state sensors in the genstate YANG data models (PTX10003)**—Junos OS Evolved Release 24.2R1 supports subscribable YANG data models for operational state on Junos devices. The genstate YANG models expose a subset of `show` command data through the gNMI subscribe RPC. A gNMI telemetry collector can subscribe to the resource paths defined in the published models to query for specific state data. This feature provides genstate YANG data model support for native physical interface state sensors.

  [See Junos Genstate YANG Data Models and gNMI Genstate Subscription.]

- **Support for native LLDP, DCBX, MVRP, and MAC rewrite sensors in genstate YANG data models (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Junos OS Evolved Release 24.2R1 supports subscribable YANG data models for operational state on Junos devices. The genstate YANG models expose a subset of `show` command data through the gNMI subscribe RPC. A gNMI telemetry collector can subscribe to the resource paths defined in the published models to query for specific state data. This feature provides genstate YANG data model support for Link Layer Discovery Protocol (LLDP), Data Center Bridging Capability Exchange (DCBX), Multiple VLAN Registration Protocol (MVRP), and Layer 2 protocol tunneling (L2PT) MAC rewrite.

  [See Junos Genstate YANG Data Models and gNMI Genstate Subscription.]

- **Support for streaming Packet Forwarding Engine statistics at the NPU-level (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Junos OS Evolved Release 24.2R1 supports streaming Packet Forwarding Engine statistics per network processing unit (NPU) and per Flexible

PIC Concentrator (FPC). Before this release, ASIC statistics were collected for all NPUs and reported as a single counter for each FPC. This feature provides refined output for ASIC counters. To stream statistics, include the FPC and NPU name in the sensor path; for example: **/components/component[name='FPC0:NPU0']/properties/property[name='hwds-normal']/**. The following leaves are supported:

- **hwds-normal**
- **hwds-data-error**
- **hwds-tcp-error**
- **hwds-illegal-nh**
- **hwds-invalid-iif**
- **hwds-fabric**

[See Junos YANG Data Model Explorer.]

- **Configure an IP source address and routing instance for legacy gRPC dial-out connections (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Junos OS Evolved Release 24.2R1 supports configuring a source IP address and routing instance for remote procedure call (gRPC) service dial-out connections. In earlier releases that support legacy gRPC dial-out, the outgoing interface IP address is used as the source address without an option to configure a source IP address. This feature supports FLEX Deployments, providing the ability to send dial-out from the router's specified IP address or interface address (such as a `loopback0` address).

  Use the `routing-instance` statement at the `[edit services analytics export-profile` *`profile-name`*`]` hierarchy level and the `local-address` *`ipv4 or ipv6 address`* statement at the `[edit services analytics export-profile` *`profile-name`*`]` hierarchy level.

  [See Using gRPC Dial-Out for Secure Telemetry Collection, routing-instance, and local-address.]

MPLS

- **Support for constraint-aware RSVP bypass LSPs (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can configure RSVP bypass LSPs to be aware of and to inherit all the path constraints from the primary LSPs. You can also explicitly configure bypass constraints for individual LSPs. With this feature, you can control the MPLS path and prevent bypass LSPs from traversing through a specific geographical area in a global MPLS RSVP network.

  [See Configuring Constraint Aware Bypass LSPs.]

- **Support for LDP dual transport over IPv4 and IPv6 sessions with NSR configuration (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR,**

PTX10003, PTX10004, PTX10008, and PTX10016)—Starting in Junos OS Evolved Release 24.2R1, you can configure the LDP dual transport mechanism to establish IPv4 and IPv6 sessions with NSR configurations. This configuration helps in forwarding IPv4 and IPv6 traffic and to support LDP IPv6 sessions in a routing instance.

[See Carrier-of-Carrier VPNs, LDP Overview, and LDP Configuration.]

- **Enable TLS for PCEP sessions (PTX10008)**—Starting in Junos OS Evolved Release 24.2R1, you can enable TLS in the Path Computation Client (PCC) to establish TCP connection with the Path Computation Element (PCE). This configuration creates a secure PCEP (PCEPS) session to transport PCEP messages.

  To enable TLS in the Path Computation Client Process (PCCD) and to establish a PCEPS session, include the `tls-strict` statement at the `[edit protocols pcep]` hierarchy level.

  [See Enabling Transport Layer Security for PCEP Sessions.]

- **Support to distribute the Entropy Label Capability (ELC) in an ISIS network (PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can distribute ELCs across all the routers in an ISIS network. ELC indicates the capability of a router to interpret Entropy Label Indicator (ELI), remove ELI/EL, and inspect next label. Entropy Readable Label Depth (ERLD) is the number of labels the router is able to read in a label stack and use it for its load balancing function. This can be used in cases of stacked labels (SR-MPLS) to insert ELs at ingress routers based on the different ELC and ERLD of the routers along its path.

  You can configure the `entropy-label` statement at the `[edit protocols isis source-packet-routing]` and at the `[edit protocols source-packet-routing source-routing-path <*>]` hierarchy levels to enable this feature. When the `entropy-label` statement is configured, the L-ISIS routes and SRTE for the prefixes are installed with a Entropy Label Indicator (ELI) if the endpoint is entropy label capable. Entropy labels are inserted only at the bottom of the label stack regardless of the ERLD of the routers along the path of the tunnel.

  The prefixes with `entropy-label-capability-flag` statement under the `prefix-attribute-flags` in the policy statement is advertised in the router to support entropy label based load balancing.

  ELC in ISIS network supports the following functionalities:

  - Store ELC in ISIS database.
  - Distribute ELC across all the routers participating in the ISIS network.
  - Propagate ELC information from ISIS database to TED.
  - Reflect ELC capability from TED in the `lsdist` table as a part of the Prefix Attribute flag.
  - Reflect ELC capability in the `lsdist` table and TED on the export side.

- Reflect the Prefix Attribute flag in ISIS, TED, and BGP LS on import and export side if `no-load-balance-label-capability` or `load-balance-label-capability` statement is configured or removed.
- Distribute ELC flag across ISIS, TED, and BGP LS if the `entropy-label-capability-flag` statement is added or removed from the policy-statement for the affected prefixes.
- Update L-ISIS routes based on the activation or deactivation of `entropy-label` statement under the [`edit protocols ISIS source-packet-routing`] hierarchy level.
- Update SR-TE routes if prefix of the tunnel endpoint is capable of doing load balancing and `entropy-label` statement is configured or removed.
- Entropy Label Capability flag is preserved when the router propagates the prefix across the ISIS levels.
- Internet, Layer 3 VPN, Layer 3 VPN, and EVPN-based services over SR and SR-TE routes using entropy-label.
- Entropy label for both IPv4 and IPv6 prefixes.
- Entropy label for SR-MPLS tunnels with IPv6 endpoint.
- Entropy label for 6PE SRTE tunnels.
- Entropy label capability advertisement for prefixes in different ISIS instance and in multi-topology.
- Entropy label for flex algorightm prefixes.
- Entropy label for source-routing-path-template.
- Entropy label for ping and traceroute to SR-TE tunnel.
- Entropy label for SBFD.

Use the `show isis database`, `show ted database`, and `show route table lsdist.0` commands to view the ELC flag in the Prefix Attribute flags. The `show route` command shows the load balancing capabilities for the L-ISIS and SPRING-TE routes with the entropy label.

The `show spring-traffic-engineering lsp detail` command displays the entropy-label capability of the tunnel only when the `entropy-label` statement is configured for the SR-MPLS in the tunnel or at the instance level.

- **Provision binding SIDs for uncolored SR-TE (SR-MPLS) LSP (PTX10008)**—Starting in Junos OS Evolved Release 24.2R1, we support provisioning of binding SID for uncolored SR-TE LSP where PCE requests PCC to allocate a binding SID from PCC's label space as follows:
  - PCE requests PCC to allocate a specific binding SID
  - PCE requests PCC to allocate binding SID of PCCs choice

We support the following PCE functionalities:

- PCE requests PCC to allocate binding SID of PCCs choice for delegated LSP.
- PCE requests PCC to allocate binding SID of PCCs choice for PCE-initiated LSP.
- PCE requests PCC to allocate a specific binding SID for delegated LSP.
- PCE requests PCC to allocate a specific binding SID for PCE-initiated LSP.
- Multiple candidate paths with binding SID in a policy.

We now support both 20-bit and 32-bit binding SID provisioned or requested from a PCE controller.

[See PCEP Configuration.]

- **Distributed CSPF support for IPv6-based SR-TE (ACX7024 and PTX10001-36MR)**—Starting in Junos OS Evolved Release 24.2R1, we support distributed CSPF path computation and auto-translation of IPv6 addresses through SR-TE configuration. A path's destination address family determines the address family of the SIDs used for the path. Configuring IPv6 addresses through SR-TE results in auto-translation of IPv6 addresses to the associated SIDs. IPv6 hops are defined in compute segment-lists.

  Use the following CLI configurations to enable auto-translation of IPv6 addresses:

```
user@host# set protocols source-packet-routing segment-list name auto-translate
user@host# set protocols source-packet-routing segment-list name name ip-address IPv6-address
```

  Use the following CLI configurations to define IPv6 hops in compute segment-lists:

```
user@host# set protocols source-packet-routing compute-profile name compute-segment-list name
user@host# set protocols source-packet-routing segment-list name compute
user@host# set protocols source-packet-routing segment-list name name ip-address IPv6-address
```

  Use the following CLI configurations to enable IPv6 path end points:

```
user@host# set protocols source-packet-routing compute-profile name …
user@host# set protocols source-packet-routing source-routing-path name to IPv6-address
user@host# set protocols source-packet-routing source-routing-path name primary name compute
compute-profile-name
```

> **NOTE:** End points must be IPv6 router IDs. Other addresses can be router IDs or interface addresses.

The `show spring-traffic-engineering lsp` command has been enhanced to show the details of IPv6 addresses.

Network Management and Monitoring

- **Clear LLDP neighbors from an interface with the gRPC Network Operations Interface (gNOI) `Layer2` service (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can execute supported `Layer2` service remote procedure calls (RPCs) to perform the equivalent of the `clear lldp neighbors interface` *`interface-name`* command.

  [See gNOI Layer 2 Service.]

- **Support for the `genstate` YANG data models (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we publish subscribable YANG data models for operational state on Junos devices. The `genstate` YANG models expose a subset of `show` command data through the gRPC Network Management Interface (gNMI) `subscribe` RPC. A gNMI telemetry collector can subscribe to the resource paths defined in the published models to query for specific state data.

  [See Junos Genstate YANG Data Models and gNMI Genstate Subscription.]

- **Support for NETCONF Call Home (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, Junos devices support the NETCONF Call Home feature for establishing a NETCONF session over SSH. NETCONF Call Home enables the Junos device to initiate a secure connection to a NETCONF client. You can use NETCONF Call Home when the NETCONF client cannot initiate a connection with the server. This situation can occur when a firewall or another security tool restricts management access to the server or implements Network Address Translation (NAT). NETCONF Call Home can also streamline the initial deployment of network devices by enabling a device to register with a management system when it is first powered on.

  [See NETCONF Call Home.]

Platform and Infrastructure

- **Restart forwarding applications for Layer 2 features (PTX10001-36MR)**—Starting in Junos OS Evolved 24.2R1, when the forwarding applications `evo-cda-bt` and `evo-aftmand-bt` restart after failure, the following forwarding applications also restart:

- packetio-bt
- ppman-aft-bt
- evoaft-jvisiond-bt
- aft-sysinfo
- fabspoked-pfe
- securityd

This behavior makes the system more resilient to abnormal termination of the evo-cda-bt and evo-aftmand-bt applications. When these forwarding applications restart, traffic forwarding stops until all applications are back to normal. In Junos OS Evolved releases before Release 24.2R1, the entire chassis would restart if either evo-cda-bt or evo-aftmand-bt failed. To manually restart the evo-cda-bt, evo-aftmand-bt, and packetio-bt applications if they ever leak memory or file handles, use the request system application *application-name* node *nodename* restart operational mode command.

[See request system application.]

Public Key Infrastructure (PKI)

- **Support for CMPv2 protocol for certificate management (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we provide support for Certificate Management Protocol (CMPv2) in the pkid process on PTX Series. Using this protocol, you can perform operations such as certificate enrollment, certificate update, and certificate loading on your device.

  [See Understanding Certificate Enrollment with CMPv2.]

- **PKI notifications support for CMPv2 protocol with jsd process (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, your PTX Series sends public key infrastructure (PKI) notification to Juniper Extension Toolkit (JET) services process (jsd) when it performs certificate management using Certificate Management Protocol (CMPv2) protocol to add, update, and clear certificate operations.

  [See Juniper Extension Toolkit Developer Guide.]

Routing Policy and Firewall Filters

- **Support for increasing firewall filter scale (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we support two new configuration statements—scale-mode and no-incremental-update. Use scale-mode to accommodate more firewall filter terms, when you're focused more on scale than on performance. Use no-incremental-update to prevent the firewall filter from undergoing incremental update; the filter undergoes make-before-break (MBB).

  [See scale-mode and no-incremental-update.]

- **Transient firewall filter for out of resource avoidance (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can configure a transient firewall filter with a presumably smaller memory footprint that performs the role of an interim firewall when its parent firewall filter is being modified.

  [See transient-filter.]

- **Support for matching IPv6 flow label field (PTX10008)**—Starting in Junos OS Evolved Release 24.2R1, support is added for matching the 20-bit `flow-label` field in the header of an IPv6 packet. We've added two new match conditions for this feature—`flow-label` *`flow label value`* and `flow-label` *`flow label value`* `mask` *`mask value`*.

  [See Firewall Filter Match Conditions for IPv6 Traffic.]

Routing Protocols

- **Support for OSPFv2 HMAC-SHA-2 keychain authentication (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can enable OSPFv2 keychain module with HMAC-SHA2 (OSPFv2 HMAC-SHA2) authentication to authenticate packets reaching or originating from an OSPF interface. HMAC SHA2 algorithms include HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 as defined in RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*. We support these algorithms along with HMAC-SHA2-224. This feature ensures smooth transition from one key to another for OSPFv2 with enhanced security. We also support HMAC-SHA1 and HMAC-SHA2 authentication for virtual and sham links.

  To enable OSPFv2 HMAC-SHA2 authentication, configure the `keychain` *`keychain-name`* configuration statement at the `[edit protocols ospf area` *`area-id`* `interface` *`interface-name`* `authentication]` hierarchy level and the `algorithm (hmac-sha2-224 | hmac-sha2-256 | hmac-sha2-384 | hmac-sha2-512)` option at the `[edit security authentication-key-chains key-chain` *`key-chain-name`*`]` hierarchy level.

  To enable keychains authentication support for OSPFv2 virtual links, configure the `keychain` *`keychain-name`* configuration statement at the `[edit protocols ospf area` *`area-id`* `virtual-link` *`neighbor-id router-id`* `transit-area area-idauthentication]` hierarchy level.

  To enable keychains authentication support for OSPFv2 sham links, configure the `keychain` *`keychain-name`* configuration statement at the `[edit protocols ospf area` *`area-id`* `virtual-link` *`neighbor-id router-id`* `transit-area area-idauthentication]` hierarchy level.

  [See Understanding OSPFv2 Authentication .]

- **Support for OSPFv2 weighted ECMP (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can enable weighted ECMP for directly connected routers. In Junos OS Evolved releases earlier than Release 24.2R1, the Junos OS Evolved ECMP algorithm does not take the underlying bandwidth into consideration. The algorithm

assumes that the links are of equal capacity, and the traffic is forwarded and distributed equally based on this assumption.

To enable weighted ECMP traffic distribution on directly connected OSPFv2 neighbors, configure the `weighted one-hop` statement at the `[edit protocols ospf spf-options multipath]` hierarchy level.

[See Understanding Weighted ECMP Traffic Distribution on One-Hop OSPF Neighbors.]

- **Support for SRLG link constraint in FAD and delay normalization (ACX Series and PTX Series)**—Starting in Junos OS Evolved Release 24.2R1, we support Flexible Algorithm Definition (FAD) defined constraints related to admin-groups and shared risk link group (SRLG) as defined in RFC 9350, *IGP Flexible Algorithm*. We also support delay normalization on the listed platforms. During Flexible Algorithm (flex algo) computation, when the measured latency values are not equal and the difference is insignificant, IS-IS advertises this slightly higher latency value as a metric. IS-IS uses this normalized latency delay value instead of the measured delay value.

  To configure flex-algo application-specific SRLG values, include the `application-specific` statement at the `[edit protocols isis interface` *`interface-name`* `level` *`level`*`]` hierarchy level.

  To exclude the SRLG constraint from an FAD, use the `exclude-srlg` statement at the `[edit routing-options flex-algorithm` *`name`* `definition]` hierarchy level.

  [See delay-measurementlevel, and definition.]

- **HMAC authentication with hash functions for IS-IS (ACX7024, ACX7100-32C, ACX7100-48L, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we extend support to IS-IS keychain with the following hash functions:

  - HMAC-SHA2-224
  - HMAC-SHA2-256
  - HMAC-SHA2-384
  - HMAC-SHA2-512

  Currently, IS-IS supports inline authentication using simple password, keyed MD5, and HMAC-SHA1 algorithms with a common keychain. Note that it's important to have the system time synchronized on all nodes when a keychain is active on an IS-IS session.

  [See **Understanding Hitless Authentication Key Rollover for IS-IS**.]

- **BGP link bandwidth community (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016, and PTX12008)**—Starting in Junos OS Evolved Release 24.2R1, BGP can communicate link speeds to remote peers, enabling better optimization of traffic distribution for load balancing. A BGP group can send the *link-bandwidth* non-transitive extended community over an EBGP session for originated or received and readvertised link-bandwidth extended communities.

To configure the non-transitive link bandwidth extended community, include the `bandwidth-non-transitive:value` in the export policy at the `[edit policy-options community name members community-ids]` hierarchy level.

To enable the device to automatically detect and attach the link-bandwidth community on a route at import, include the `auto-sense` statement at the `[edit protocols bgp group link-bandwidth]` hierarchy level. This feature facilitates the integration of devices with different transmission speeds within the network, enabling efficient traffic distribution based on link speed.

[See auto-sense, and group (Protocols BGP).]

- **Enable RFC 7606-based error handling in BGP (PTX10008)** —Starting in Junos OS Evolved Release 24.2R1, we support RFC 7606, *Revised Error Handling for BGP UPDATE Messages* that revises the BGP error handling by default. If the errors can be tolerated, BGP recommends that you use the attributes `discard` and `treat-as-withdraw` instead of a session reset. However, if the errors are too severe, BGP triggers a session reset. The session reset minimizes the impact of a malformed update message on routing by retaining the established sessions and valid routes.

  The `bgp-error-tolerance` statement at `[edit protocols bgp]`hierarchy level is enabled by default. You can still configure suboptions such as `malformed-route-limit`, `malformed-update-log-interval`, and `no-malformed-route-limit` under this configuration statement. Note that If you delete the `bgp-error-tolerance` statement, the feature will still remain enabled, but the suboptions are reset to their default values.

  [See bgp-error-tolerance (Protocols BGP).]

- **Support for BGP VPN to global RIB import (PTX10001-36MR)**—Starting in Junos OS Evolved Release 24.2R1, we support leaking of BGP VPN routes to global routing information bases (RIBs) to provide service providers the flexibility to allow Internet access to VPN customers. To configure this feature, include the `vpn-global-import policy` statement at the `[edit routing-options inet.0]` hierarchy level.

  To use the automatic router discovery feature with the router ID without allocating an IP-address, include the `route-distinguisher-id-use-router-id` statement at the `[edit routing-options]` hierarchy level.

  [See route-distinguisher-id-use-router-id, and vpn-global-import.]

- **Support for configuring multiple independent IGP instances of OSPFv2 (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can configure and run multiple independent IGP instances of OSPFv2 simultaneously on a router as defined in RFC 6549, *OSPFv2 Multi-Instance Extensions*.

  With this feature:

  - You can use multiple IGP instances of OSPFv2 to redistribute routes among independent OSPFv2 domains on a single router.
  - You can construct flexible OSPFv2 hierarchies across independent IGP domains.

- You can achieve a more scalabale OSPFv2 deployment.

To enable multiple IGP instances of OSPFv2 routing on the routing device, configure `ospf-instance` *`igp-instance-name`* at the `[edit protocols ospf]` hierarchy level.

> **NOTE**: Junos OS Evolved does not support configuring the same logical interface with multiple IGP instances of OSPFv2.

[See Multiple Independent IGP Instances of OSPFv2 Overview.]

- **Support IPv6 address for seamless BFD over static segment routing MPLS LSPs (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, PTX Series devices support the IPv6 address family for seamless Bidirectional Forwarding Detection (S-BFD) over static segment routing MPLS LSPs. The mode of operation for sBFD support for IPv6 in centralized and distributed mode is as follows:

  - IPv6 support for sBFD over static segment routing MPLS LSP for responder and initiator in distributed mode.
  - IPv6 support for sBFD over static segment routing MPLS LSP for initiator in centralized mode.

  You can configure the sBFD IPv6 responder session only by including the `local-ipv6-address` statement at the `[edit protocols bfd sbfd local-discriminator disc]` hierarchy level as follows:

```
user@host# set protocols bfd sbfd local-discriminator disc local-ipv6-address ipv6-address
```

  The configured IPv6 address is used as the source IPv6 address in the reply packet.

Serviceability

- **On-device packet capture (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, Junos devices support filtering and mirroring incoming and outgoing packets, sending those packets to the CPU, and saving them into a file. This feature, *on-device packet capture*, can help you with protocol and application analysis, debugging, troubleshooting, network forensics, audit trails, and network attack detection. On-device packet capture (or “self-mirroring”) sends the sampled copy to a CPU and writes the copy into a packet capture (**.pcap**) file. The process does not require you to use any device connected to your network device.

  More about on-device packet capture:

  - Operational commands allow you to start and stop the capture.
  - `family` is an optional parameter, and the families you can specify are `inet`, `inet6`, and `any`.

- You can specify the write mode of the packet capture file—either circular (the default) or linear.
- `rate` and `max-packet-length` properties apply to self-mirroring.
- You can configure both “standard” port mirroring and self-mirroring on your device—you just need to ensure that you don't configure an individual port-mirroring instance for both mirroring types.

[See On-Device Packet Capture.]

- **Support for enhanced request support information (ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we've deprecated the CLI option `brief` from the `request support information` command and introduced the following CLI options to the existing `request support information` command:
  - `archive`
  - `with-logs`
  - `with-components`
  - `with-options`.

  [See request support information.]

Services Applications

- **Export of IPFIX and version 9 records of sampled packets through the management interface and WAN ports belonging to the non-default VRF instance (PTX Series)**—Starting in Junos OS Evolved Release 24.2R1, we support export of IPFIX or version 9 records of inline active flow monitoring sampled packets to collectors reachable through:
  - Interfaces belonging to the mgmt_junos VRF instance.
  - WAN ports belonging to the non-default VRF instance.

  You configure this feature using the `routing-instance` configuration statement at the `[edit forwarding-options sampling instance` *`name`* `family` *`type`* `flow-server` *`IP-address`*`]` hierarchy level. You must ensure that the collectors are reachable through the management interface. We support a maximum of four collectors for each type of VRF instance. You can configure collectors for both types of VRF instances in the same sampling configuration. However, the collectors reachable through the mgmt_junos VRF instance and the collectors reachable through the WAN ports cannot coexist under the same family, because you can specify only one source IP address per family. You can specify `inet` collectors, `inet6` collectors, or a mix of the two types.

  [See Configuring Inline Active Flow Monitoring on PTX Series Routers and routing-instance (Flow Monitoring).]

Software Installation and Upgrade

- **Base OS update (ACX Series and PTX Series)**—Starting in Junos OS Evolved Release 24.2R1, Junos OS Evolved uses the Wind River Linux LTS 22 base OS. This upgrade provides improved security and better performance. In earlier releases, Junos OS Evolved used the Wind River Linux LTS 19 base OS.

- **Migrate to GPT disk partitioning (ACX Series and PTX Series)**—Starting in Junos OS Evolved Release 24.2R1, we support migrating to GUID Partition Table (GPT) disk partitioning. GPT is the native disk partitioning scheme used by UEFI BIOSes. GPT is similar to the Master Boot Record (MBR) disk partitioning scheme used by traditional BIOSes. All Junos OS Evolved platforms support GPT natively. However, we default to MBR disk partitioning because Junos OS Evolved was originally ported to systems that used traditional BIOSes.

  GPT has several advantages over MBR:

  - Support for much larger disks
  - Unique partition ID support by using GUIDs
  - Human-readable partition names
  - Backup copies

  When you install a release that supports GPT disk partitioning, you can:

  - For new installations, change the default partition scheme for both the primary and secondary disks to GPT immediately (for example, scratch installations to empty disks).
  - For existing installations, migrate to GPT disk partitioning for both the primary and secondary disks after a reboot of the system.

  [See Software Installation and Upgrade Overview (Junos OS Evolved).]

- **Support for SZTP (ACX7100-32C, ACX7100-48L, PTX10004, PTX10016, and PTX10001-36MR)**—Starting in Junos OS Evolved Release 24.2R1, you can use RFC-8572-based secure zero-touch provisioning (SZTP) to bootstrap your remotely located network devices that are in a factory-default state. SZTP enables mutual authentication between the bootstrap server and the network device before the remote network device is accessed for initiating ZTP.

  To enable mutual authentication, you need a unique digital voucher, which is generated based on the DevID (digital device ID or cryptographic digital identity) of the network device. The DevID is embedded inside the Trusted Platform Module (TPM) 2.0 chip ONLY on ACX7100-48L-*xxx*-K, ACX7100-32C-*xxx*-K, and PTX10001-36MR-K network devices. Juniper Networks issues a digital voucher to customers for each eligible network device.

  [See Secure Zero Touch Provisioning.]

-

- **Support for executing a pre-upgrade script with SZTP (ACX7024, ACX7100-32C, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can execute a pre-upgrade script to download signing keys or certificates for your third-party applications before provisioning your device. You can use the `pre-upgrade-script` XML tag to provide a pre-upgrade script as part of your onboarding information for SZTP.

  [See Secure Zero Touch Provisioning.]

- **Support for executing a pre-upgrade script with ZTP (ACX7024, ACX7100-32C, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can execute a pre-upgrade script to download signing keys or certificates for your third-party applications before provisioning your device. You can also use a pre-upgrade script to specify the management and WAN interface names and the speed of the WAN interfaces for ZTP. ZTP uses this information to avoid cycling through the unnecessary speed groups where the interface does not reside.

  You can use DHCP option 43 suboption 9 for DHCPv4 and DHCP option 17 suboption 9 for DHCPv6 to specify the name of your pre-upgrade script as part of the bootstrap information. You can also toggle the behavior for DHCPv4 option 43 suboption 5 to specify either the IP address of the FTP server or the HTTP port.

  [See Zero Touch Provisioning.]

- **Support for HTTP and HTTPS authentication on ZTP (ACX7024, ACX7100-32C, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can enable basic HTTP and HTTPS authentication for IPv4 and IPv6.

  To enable basic HTTP and HTTPS authentication for IPv4, use DHCP option 43 suboption 3. IPv6 ignores this option.

  For IPv6, provide the authentication parameters through the boot file URL and the URLs for the image, configuration, and alternate image. The precedence is the URL for the image, followed by the configuration, and then the alternate image. After that, the boot file URL is used. For authentication, the transfer type needs to be either HTTP or HTTPS.

  [See Zero Touch Provisioning.]

- **Support for HTTP and HTTPS proxy server on ZTP (ACX7024, ACX7100-32C, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, you can now configure an HTTP or HTTPS proxy server for ZTP.

  To specify an HTTP or HTTPS proxy server for IPv4, use DHCP option 43 suboption 8.

  To specify an HTTP or HTTPS proxy server for IPv6, use DHCP option 17 suboption 8.

  [See Zero Touch Provisioning.]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **BGP classful transport support for dynamic tunnels and colored transport-rib for next-hop-based tunnels (PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016)**—Starting in Junos OS Evolved Release 24.2R1, we support the colored transport RIB model for next-hop-based dynamic tunnels. By default, GRE tunnels are logical interface-based tunnels. IPIP and UDP tunnels are next-hop based tunnels. GRE tunnels can also be configured as next-hop based tunnels by including the GRE `next-hop-based-tunnel` statement at the [`edit routing-options dynamic-tunnels`] hierarchy level.

  For logical interface and next-hop-based tunnels, dynamic tunnel specific route addition is triggered when an application route with protocol next-hop is resolved on dynamic tunnel catch-all route.

  To support the colored transport-rib model for DTM next-hop based tunnels, configure the `use-transport-class` statement under the [`edit dynamic-tunnels` *`tunnel-name`*] configuration. If you don't configure the `use-transport-class` statement, then a catch-all route and an application route are created in the inet(6)color.0 table. If you configure the `use-transport-class` statement, then the catch-all route and the application route are created in the color.inet(6).3 table. If you include the `best-effort` statement at the [`edit routing-options dynamic-tunnels` *`dynamic-tunnel-name`* `destination-networks` *`ip-address`*] hierarchy level, dynamic tunnels are created in the inet(6)color.0 table.

  To enable the `use-transport-class` statement under the dynamic-tunnel configuration, include the `auto-create` statement at the [`edit routing-options transport-class`] hierarchy level.

  To configure a colored transport-rib, include the `preserve-nexthop-hierarchy` statement at the [`edit routing-options resolution`] hierarchy level.

- **Support for IPv6 endpoints for SR-MPLS DTM SR-TE tunnels (PTX10001-36MR)**—Starting in Junos OS Evolved Release 24.2R1, we support IPv6 end points for SR-MPLS DTM SR-TE tunnels. You can configure IPv6 destination networks under SPRING-TE dynamic tunnels and support dynamic segment lists and distributed Constrained Shortest Path First (using compute-profile). We support the following SR-TE dynamic tunnel models:

  - IPv6 endpoint for DTM uncolored SR-TE tunnels
  - IPv6 endpoint for DTM SR-TE tunnels (SR-MPLS) with inet6color.0 model
  - IPv6 endpoint for DTM SR-TE tunnels (SR-MPLS) with transport-rib model

  To support the transport-rib model for IPv6 DTM SR-TE tunnels, include the `use-transport-class` statement at the [`edit dynamic-tunnels` *`tunnel-name`* `spring-te`] hierarchy level.

  If the `use-transport-class` statement is not configured, then the catch-all route and the application route are created in the inet6color.0 table. If the `use-transport-class` statement is configured, then the catch-all route and the application route are created in the color.inet6.3 table. This behavior is irrespective of using the `use-transport-class` statement at the [`edit protocols source-packet-routing`] hierarchy level. For DT tunnels, SR-TE takes preference of the `use-transport-class` statement at the

[edit dynamic-tunnels *tunnel-name* spring-te] hierarchy rather than at the [edit protocols source-packet-routing] hierarchy level.

Additional Features

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

- **Fast lookup filter** (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)—Support extended to ethernet switching, any, mpls, and ccc firewall filter families for fast lookup filters on PTX Series routers.

  [See fast-lookup-filter (PTX).]

- **Firewall filter support for bitwise logical operations for TCP Flag match** (PTX10004, PTX10008, and PTX10016)

  [See Firewall Filter Match Conditions Based on Bit-Field Values.]

- **Juniper Resiliency Interface** (PTX10003) You can use the Juniper Resiliency Interface (JRI) to detect, correlate, and mitigate routing exceptions.

  [See Juniper Resiliency Interface.]

- **Layer 2 pseudowire redundancy** (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)

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

- **Seamless EVPN-VXLAN to EVPN-VXLAN stitching** (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)

  [See interconnect.]

- **Support for EVPN E-LAN over SRv6 underlay** (ACX7024X and ACX7332)

  [See Configuring EVPN E-LAN over SRv6.]

- **Support for filter-based forwarding** (PTX10004, PTX10008, and PTX10016)

  [See Example: Configuring Filter-Based Forwarding to a Specific Outgoing Interface or Destination IP Address.]

- **Support for file system encryption with Trusted Platform Module (TPM 2.0)** (ACX7100-32C, ACX7100-48L, PTX10001-36MR, PTX10004, PTX10008, and PTX10016)

  [See Encryption with TPM.]

- **Support for firewall filter based de-encapsulation (IP-IP)** (PTX10004 and PTX10008

  [See Configuring a Filter to De-Encapsulate IPIP Traffic.]

- **Support for MAC-VRF in EVPN multihomed environment** (PTX10001-36MR, PTX10004, PTX10008, and PTX10016)

  [See Configuring EVPN-MPLS Active-Standby Multihoming.]

- **Support for monitoring MPLS LSP** (ACX7024, ACX7024X, ACX7100, ACX7332, ACX7348, ACX7509, PTX10004, PTX10008, PTX10016, PTX10001-36MR, and PTX10003, and the PTX10000-LC1202 line card)

  [See LSP Labels.]

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

- **400ZR and 400G OpenZR+ support enhancements** (PTX10004, PTX10008, and PTX10016). The enhancements include application selection and configuration of target output power. You can view the advertised applications and switch between the applications.

  [See 400ZR and 400G OpenZR+.]

-

What's Changed

IN THIS SECTION

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

Authentication and Access Control

- **ChaCha20-Poly1305 algorithm deprecation for SSH cipher option**— The ChaCha20-Poly1305 authenticated encryption algorithm is deprecated for SSH cipher option. Configure aes-128-gcm and aes-256-gcm as the encryption algorithm for SSH Cipher option. [See ssh (System Services).]

EVPN

- **OISM SBD bit in EVPN Type 3 route multicast flags extended community**—In EVPN Type 3 Inclusive Multicast Ethernet Tag (IMET) route advertisements for interfaces associated with the supplemental bridge domain (SBD) in an EVPN optimized intersubnet multicast (OISM) network, we now set the SBD bit in the multicast flags extended community. We set this bit for interoperability with other vendors, and to comply with the IETF draft standard for OISM, draft-ietf-bess-evpn-irb-mcast. You can see this setting in the output from the `show route table bgp.evpn.0 ? extensive` command.

  [See CLI Commands to Verify the OISM Configuration.]

- **Group-based Policy (GBP) tag displayed with `show bridge mac-table` command**—On platforms that support VXLAN-GBP, the `show bridge mac-table` command now displays a GBP TAG output column that lists the GBP tag associated with the MAC address for a bridge domain or VLAN in a routing instance. Even if the device does not support or not using GBP itself, the output includes this information for GBP tags in packets received from remote EVPN-VXLAN peers.

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

- **Updates to syslog EVPN_DUPLICATE_MAC messages**—EVPN_DUPLICATE_MAC messages in the System log (syslog) now contain additional information to help identify the location of a duplicate

MAC address in an EVPN network. These messages will include the following in addition to the duplicate MAC address:

- The peer device, if the duplicate MAC address is from a remote VXLAN tunnel endpoint (VTEP).
- The VLAN or virtual network identifier (VNI) value.
- The source interface name for the corresponding local interface or multihoming Ethernet segment identifier (ESI).

For example: `Feb 27 22:55:13 DEVICE_VTEP1_RE rpd39839: EVPN_DUPLICATE_MAC: MAC address move detected for 00:01:02:03:04:03 within instance=evpn-vxlan on VNI=100 from 10.255.1.4 to ge-0/0/1.0.`

For more on supported syslog messages, see System Log Explorer.]

- **New commit check for MAC-VRF routing instances with the `encapsulate-inner-vlan` statement configured**— We introduced a new commit check that prevents you from configuring an IRB interface and the `encapsulate-inner-vlan` statement together in a MAC-VRF routing instance. Please correct or remove these configurations prior to upgrading to 23.2R2 or newer to avoid a configuration validation failure during the upgrade.

  [See encapsulate-inner-vlan.]

- **Default behavior changes and new options for the easy EVPN LAG configuration (EZ-LAG) feature**— The easy EVPN LAG configuration feature now uses some new default or derived values, as follows:
  - Peer PE device `peer-id` value can only be 1 or 2.
  - You are required to configure the loopback subnet addresses for each peer PE device using the new `loopback peer1-subnet` and `loopback peer2-subnet` options at the **edit services evpn device-attribute** hierarchy level. The commit script uses these values for each peer PE device's loopback subnet instead of deriving those values on each PE device. These replace the `loopback-subnet` option at the **edit services evpn device-attribute** hierarchy level, which has been deprecated.
  - If you configure the `no-policy-and-routing-options-config` option, you must configure a policy statement called EXPORT-LO0 that the default underlay configuration requires, or configure the new `no-underlay-config` option and include your own underlay configuration.
  - The commit script generates "notice" messages instead of "error" messages for configuration errors so you can better handle **edit services evpn** configuration issues.
  - The commit script includes the element names you configure (such as IRB instance names and server names) in description statements in the generated configuration.
  - This feature also now includes a few new options so you have more flexibility to customize the generated configuration:

- `no-underlay-config` at the **edit services evpn** hierarchy level—To provide your own underlay peering configuration.

- `mtu overlay-mtu` and `mtu underlay-mtu` options at the **edit services evpn global-parameters** hierarchy level—To change the default assigned MTU size for underlay or overlay packets.

- **Limit on number of IP address associations per MAC address per bridge domain in EVPN MAC-IP database**—By default, devices can associate a maximum of 200 IP addresses with a single MAC address per bridge domain. We provide a new CLI statement to customize this limit, `mac-ip-limit` statement at the **edit protocols evpn** hierarchy level. In most use cases, you don?t need to change the default limit. If you want to change the default limit, we recommend that you don?t set this limit to more than 300 IP addresses per MAC address per bridge domain. Otherwise, you might see very high CPU usage on the device, which can degrade system performance.

  See [mac-ip-limit.]

See [Easy EVPN LAG Configuration.]

Flow-based and Packet-based Processing

- The subscription path for the flow sensor is changed from /junos/security/spu/flow/usage to /junos/security/spu/flow/statistics. This change maintains a uniform path in request and response data.

General Routing

- **Enhanced DDoS status operational command (PTX Series)**—We've enhanced the aggregate DDoS status output field to display the aggregate count of all sub packet types.

  Earlier to this release, the aggregate DDoS status output displayed only the packet type level output information.

  [See show ddos-protection protocols.]

- The `show chassis fabric topology` command displays interleaved source and destinations tags in In-Links and Out-Links output fields for PTX series devices in Junos Evolved release versions 21.4R1 and later.

- On PTX10004, PTX10008, and PTX10016 routers, after executing the `request node offline` command, you must wait at least 180 seconds to execute the `request chassis cb offline` command.

- Media Access Control Security (MACsec) session remains stable when changing exclude-protocol configuration—When you change the protocols excluded from MACsec using the exclude-protocol

protocol-name option at the **edit security macsec connectivity-association connectivity-association-name**, the MACsec session remains stable.

[See exclude-protocol.]

- **Enhanced DDoS statistics operational command (PTX Series)**—We've enhanced the aggregate DDoS statistics output field to display the aggregate statistics for BFD and DHCP protocols. The enhanced DHCP statistics output displays the collective DHCPv4 and DHCPv6 statistics for DDoS.

  Earlier to this release, the aggregate DDoS statistics output displayed 0 for aggregate BFD and the aggregate DHCPv4v6.

- **Change in options and generated configuration for the EZ-LAG configuration IRB subnet-address statement**—With the EZ-LAG `subnet-address inet` or `subnet-address inet6` options at the **edit services evpn evpn-vxlan irb *irb-instance*** hierarchy, you can now specify multiple IRB subnet addresses in a single statement using the list syntax **addr1 addr2 ...** . Also, in the generated configuration for IRB interfaces, the commit script now includes default `router-advertisement` statements at the **edit protocols** hierarchy level for that IRB interface.

  See [subnet-address (Easy EVPN LAG Configuration).]

- The command request system zeroize has been updated to securely erase ATA disks on Routing Engines. This update makes it difficult to access data on the disks, using various levels of sanitization corresponding to degrees of difficulty, as defined in the NIST 800-88 standard. If the Routing Engine contains two disks, you can now sanitize the disks one at a time, using the disk1 or the disk2 option.

- **DDoS violation information shows incorrect default time and date (PTX Series)**—When you clear the DDoS violation state using the `clear ddos-protection protocols states` command in Junos OS Evolved, the log message displays an incorrect default time and date. However, if you bypass the recovery time while clearing the DDoS violation state, the log message displays accurately.

  See [clear ddos-protection protocols.]

- The system now checks the port number value (z) in the 'set interfaces et-x/y/z:n' configuration for a valid port range on PTX10002-36QDD. Previously, configurations with invalid port numbers were committed successfully. With this update, the system displays a UI error message and prevents committing configurations with invalid port numbers, ensuring configuration accuracy and preventing potential issues.

- Three new VSA's have been added to code repository for 802.1x authentication on RADIUS server under Vendor ID: 2636: - 53: Event-Type - 54: Sub-Event-Type - 55: Juniper-Generic-Message

  See [Radius Attributes and VSA list supported by 802.1X.]

- **Change to the commit process**—In prior Junos OS Evolved releases, if you use the commit prepare command and modify the configuration before activating the configuration using the commit activate command, the prepared commit cache becomes invalid due to the interim configuration change. As a

result, you cannot perform a regular commit operation using the commit command. The CLI shows an error message: 'error: Commit activation is pending, either activate or clear commit prepare'. If you now try running the commit activate command, the CLI shows an error message: 'error: Prepared commit cache invalid, failed to activate'. You then must clear the prepared configuration using the clear system commit prepared command before performing a regular commit operation. From this Junos and Junos OS Evolved release, when you modify a device configuration after 'commit prepare' and then issue a 'commit', the OS detects that the prepared cache is invalid and automatically clears the prepared cache before proceeding with regular 'commit' operation.

See [Commit Preparation and Activation Overview .]

- Disabled CDN auto download (Junos OS Evolved) — The PKI process periodically, by default every 24 hours, polls the CDN server for the latest default trusted CA bundle and updates the list for any changes to the trusted CAs in the bundle. If there are any changes, PKI process loads them in the background. The auto download of CA certificates might generate core files. We've disabled the service of PKI query to CDN server periodically to download the latest trusted CA bundle.

- **Feature bandwidth information in CLI output (PTX Series)**—Starting in this release, the `show system license` command output displays bandwidth only if an IFL and Advance or Premium features are configured.PR1783572

- ChaCha20-Poly1305 algorithm deprecation for SSH cipher option - The ChaCha20-Poly1305 authenticated encryption algorithm is deprecated for SSH cipher option. Configure aes-128-gcm and aes-256-gcm as the encryption algorithm for SSH Cipher option.

  [See ssh (System Services).]PR1783811

- New CLIs introduced to collect Layer 2 bridging and Layer 2 protocols for smart debugging.PR1791299

- Remote port-mirroring configuration error messages (PTX10002-36QDD)—When you configure remote port-mirroring and restart the Packet Forwarding Engine (PFE), syslog displays error messages indicating unbind failures.PR1800337

- Corrected show ddos-protection protocols CLI command (PTX10003, PTX10008, and PTX10016)—When you clear the DDoS state and then execute the `show ddos-protection protocols` CLI command, the output accurately displays that the policer was never violated. Earlier to this release, the `show ddos-protection protocols` CLI command output displayed that the policer was no longer violated, which indicates that violation occurred and wasn't cleared correctly.

  [See show ddos-protection protocols.]

Infrastructure

- **Option to disable path MTU discovery**—Path MTU discovery is enabled by default. To disable it for IPv4 traffic, you can configure the `no-path-mtu-discovery` statement at the [`edit system internet-options`] hierarchy level. To reenable it, use the `path-mtu-discovery` statement.

  [See Path MTU Discovery.]

Interfaces and Chassis

- **Disable power redundancy alarms for JNP10K-PWR-DC2 PSM (PTX10008 and PTX10016)**— The JNP10K-PWR-DC2 PSM supports power redundancy across two DIP switches. When all input feeds are not connected to power supplies, it triggers a chassis alarm such as `PSM 5 Input B0 and B1 Failed`. Starting in Junos OS Evolved Release 24.2R1, you can disable this chassis alarm by using the `set chassis alarm psm` *`psm number`* `input` *`input number`* `ignore` command.

  [See JNP10K-PWR-DC2 Power Supply.]

- **Zeroize a specific disk**—The Routing Engine of your device has multiple disks for redundancy. Use the command `request system zeroize (disk1|disk2)` to zeroize only one of the disks. Use `disk1` to zeroize the primary disk (/dev/sda) and `disk2` to zeroize the backup disk (/dev/sdb).

  [See request system zeroize (Junos OS Evolved).]

Junos Node Slicing

- **Change in the XML tags displayed for the `show virtual-network-functions` command in JDM (Junos node slicing)**—To align the XML tags displayed for the `show virtual-network-functions` *`gnf-name`* `| display xml` with the new XML validation logic, we have replaced the underscores (_) in the output with hyphens (-) as shown below:

  Old output:

```
user@jdm> show virtual-network-functions mgb-gnf-d | display xml
<rpc-reply xmlns:junos=http://xml.juniper.net/junos/23.4I0/junos>
    <vnf-information xmlns=http://xml.juniper.net/junos/23.4I0/junos-jdmd
junos:style="detail">
        <vnf-instance>
            <id>1</id>
```

```
            <name>mgb-gnf-d</name>
            <state>Running</state>
            <liveliness>down</liveliness>
            <ip_addr>192.168.2.1</ip_addr>  <<< The tag includes _.
            <vcpus>2</vcpus>
            <max_mem>16GiB</max_mem>  <<< The tag includes _.
            <resource_template>2core-16g</resource_template>   <<<  The tag includes _.
            <qemu_process_id>614702</qemu_process_id>    <<<  The tag includes _.
            <smbios_version>v2</smbios_version>             <<<  The tag includes _.
            <vnf-blk-dev-list>
            </vnf-blk-dev-list>
        </vnf-instance>
    </vnf-information>
    <cli>
        <banner></banner>
    </cli>
</rpc-reply>
```

New output:

```
user@jdm> show virtual-network-functions mgb-gnf-d | display xml
<rpc-reply xmlns:junos=http://xml.juniper.net/junos/23.4I0/junos>
    <vnf-information xmlns=http://xml.juniper.net/junos/23.4I0/junos-jdmd
junos:style="detail">
        <vnf-instance>
            <id>1</id>
            <name>mgb-gnf-d</name>
            <state>Running</state>
            <liveliness>down</liveliness>
            <ip-addr>192.168.2.1</ip-addr>  <<< The tag changes to ip-addr.
            <vcpus>2</vcpus>
            <max-mem>16GiB</max-mem>  <<< The tag changes to max-mem.
            <resource-template>2core-16g</resource-template>   <<< The tag changes to
resource-template.
            <qemu-process-id>614702</qemu-process-id>    <<< The tag changes to qemu-process-
id.
            <smbios-version>v2</smbios-version>             <<< The tag changes to smbios-
version.
            <vnf-blk-dev-list>
            </vnf-blk-dev-list>
        </vnf-instance>
    </vnf-information>
```

```
    <cli>
        <banner></banner>
    </cli>
</rpc-reply>
```

This change is applicable to any RPC that previously had underscores in the XML tag name.

Junos OS API and Scripting

- **<get-trace> RPC support removed (ACX Series and PTX Series)**—The `show trace application` *app-name* operational command and equivalent `<get-trace>` RPC both emit raw trace data. Because the `<get-trace>` RPC does not emit XML data, we've removed support for the `<get-trace>` RPC for XML clients.

Multicast

- **Non-revertive switchover for sender based MoFRR**— In earlier Junos releases, source-based MoFRR ensured that the traffic reverted to the primary path from the backup path, when the primary path or session was restored. This reversion could result in traffic loss. Starting in Junos OS Evolved 22.4R3-S1, source-based MoFRR will not revert to the primary path, i.e. traffic will continue to flow through the backup path as long as the traffic flow rate on the backup path does not go below the configured threshold set under `protocols mvpn hot-root-standby min-rate`.

  [See min-rate.]

Network Management and Monitoring

- With this release, the CLI does not allow you to delete the `?management-instance?` configuration from the **edit system** hierarchy level if you have configured syslog messages for remote hosts with the `?mgmt_junos?` instance as routing instance at the **edit system syslog** hierarchy level and at the **edit system** hierarchy level. If you try to delete the management-instance configuration at the **edit system** hierarchy level without deleting it from the **edit system syslog** hierarchy level, the CLI shows a commit error.PR1785475

- **Change in use of RSA signatures with SHA-1 hash algorithm**—Starting in Junos OS Release 24.2R1, there is a behavioural change by OpenSSH 8.8/8.8p1. OpenSSH 8.8/8.8p1 disables the use of RSA signatures with SHA-1 hash algorithm by default. You can use RSA signatures with SHA-256 or SHA-512 hash algorithm.

Platform and Infrastructure

- Starting Junos Evolved Release 24.2R1, support for Network Time Protocol (NTP) over TLS (RFC 8915 compliant) for the ACX-series and PTX-series includes:
  - Support to configure local-certificate for server and certificate verification option for client.
  - Verification of x.509 certificates to establish a TLS channel between client and server. - TLS NTS-KE protocol support.
  - Support for NTS secured client-server NTP communication at server and client.
  - Support for new NTS options in commands `system ntp nts`, `system ntp server <server_name> nts remote-identity`, and `show ntp associations no-resolve` commands.

System Management

- **Additional `Upgrade` fields for the `show system applications detail` command (ACX Series and PTX Series)**—The `show system applications detail` command and corresponding RPC include additional `Upgrade` output fields. The fields provide information about notifications and actions related to various upgrade activities.

  [See show system applications (Junos OS Evolved).]

User Access and Authentication

- Starting in Junos OS Release 24.2R1 and Junos OS Evolved Release 24.2R1, when you run the run `show lldp local-information interface <interface-name> | display xml` command, the output is displayed under the **lldp-local-info root** tag and in the **lldp-local-interface-info container** tag. When you run the run `show lldp local-information interface | display xml` command, the **lldp-tlv-filter** and **lldp-tlv-select** information are displayed under the **lldp-local-interface-info container** tag in the output.
- **Viewing files with the `file compare files` command requires users to have `maintenance` permission**—The `file compare files` command in Junos OS Evolved requires a user to have a login class with `maintenance` permission.

  [See Login Classes Overview.]

User Interface and Configuration

- **Viewing files with the `file compare files` command requires users to have `maintenance` permission**—The `file compare files` command in Junos OS and Junos OS Evolved requires a user to have a login class with `maintenance` permission.

  [See Login class overview.]

VPNs

- **Increase in revert-delay timer range**— The `revert-delay` timer range is increased to 600 seconds from 20 seconds.

  [See min-rate.]

- **Configure min-rate for IPMSI traffic explicitly**— In a source-based MoFRR scenario, you can set a min-rate threshold for IPMSI traffic explicitly by configuring `ipmsi-min-rate` under `set routing-instances protocols mvpn hot-root-standby min-rate`. If not configured, the existing `min-rate` will be applicable to both IPMSI and SPMSI traffic.

  [See min-rate.]

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.

Routing Policy and Firewall Filters

- Supported maximum bit length on the platform is 24 bits with respect to flexible mask range. Hence,the bit length 32 does not hold valid in this case. PR1798923

Open Issues

IN THIS SECTION

Learn about open issues in this release for PTX Series routers

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

General Routing

- G.8273.2 Synce to PTP and SyncE to 1PPS Transient Response test fails. PR1681527
- Class B performance as per G.8273.2 fails for SyncE to PTP and SyncE to 1pps Noise transfer for lower frequencies. PR1681884
- Class B performance as per G.8273.2 might be supported only when FEC gets enabled on both the primary and slave ports of the T-BC(default option). PR1683579
- The fan FRU does not get displayed in the SNMP queries. Only FT and FTC gets displayed. This is in comparison MX device which also gets displayed as FAN also and its status in SNMP FRU. PR1754833
- The modification of the values for the following leaves under queue-management-profiles does not support drop weight enable-ecn. The support for this modification functionality requires feature enhancement. The proposed workaround for this is 1. Delete the entire queue-management-profile 2. Reconfigure with the new updated parameters. PR1769922

- With DHCP trace options enabled in their regression scripts, core file gets generated. This isue is randomly not seen always. This was enabled in script for debugging in production network this will not be enabled by default hence the issue will not be seen. Its recommended to enable DHCP trace options only for debugging not otherwise. PR1771121

- As per OpenSSH 9.0/9.0p1 release notes, this release switches scp(1) from using the legacy scp/rcp protocol to using the SFTP protocol by default. Hence, Junos OS Evolved running OpenSSH 9.0 and above will use the "SFTP" protocol by default when scp command is invoked from shell. However, Junos OS Evolved running OpenSSH 9.0 and above will use the "SCP" protocol by default when scp command is invoked from the Juniper CLI. The scp command in the Juniper CLI will also be updated to use the "SFTP" protocol by default in a release later than 24.2R1-EVO. In case a user is required to use the "SCP" protocol from shell, please use the -O command line option to switch scp to "SCP" protocol. For example: scp -O other options arguments Note: Incoming SCP connections from outside hosts that are running OpenSSH version >=9.0/9.0p1 could fail since sftp-server is disabled by default in Junos OS Evolved. Hence, users should either use the -O option on remote host while initiating scp file transfer OR enable sftp-server in the Juniper configuration. To enable sftp-server in Juniper configuration, use the `set system services ssh sftp-server` hierarchy. PR1787659

- A rare core might get generated in the firewall consumer `kfirewall-agent` and `fwstatsd` applications while repeatedly making configuration changes related to interfaces and firewalls. After the applications generates core files, the applications restarts and functions normally. PR1818196

- 1. To avoid a PSU ending up on "Unsupported" state, when a PSU is inserted into a live system, it **must be** pushed completely in (a little bit beyond the point when LEDs light up), and the thump screw must be tightened completely for proper operation. 2. If a PSU gets into the **unsupported** state, it can be slightly pulled out, and re-inserted completely after 30 seconds. This will fix the issue. 3. Alternatively, after all the PSUs are completely inserted into the system with their thumb-screws completely tightened, a chassis-level power cycle will result in detection of all PSUs correctly.PR1784345

Network Management and Monitoring

- On Junos OS Evolved platforms, SNMP cold start trap occurs on the console log upon system reboot but does not sent out to the external server. PR1788308

Routing Policy and Firewall Filters

- On PTX devices running Junos OS Evolved Release 22.2R3-S3, the commit check fails with `checkloFilterBindingListCallback` when trying to apply filters on lo0 interface. PR1800262

Resolved Issues

IN THIS SECTION

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)

- Deletion of classifier or rewrite with import statement along with some extra rules leads to the cosd process crashes. PR1787101

EVPN

- In the EVPN-MPLS scenario, traffic between the CE devices drop. PR1786959

General Routing

- On PTX10008 PTP-PTP and PTP-1pps, few frequencies might fail to meet the mask. PR1624478
- On PTX1003 devices, High Scale for SPMSI NGMVPN is not supported. PR1708454

- The pkid process fails during restart. PR1729592
- We might encounter jdhcpd core files during initialization. The core in rare, and there is no service impact because of this core as the process recovers immediately. PR1730717
- Observing continuous ssh errors on log messages gets generated: `(error: Could not load host key: /etc/ssh/ssh_host_ec_p521_key)`. PR1744354
- The license-check can get restarted. PR1760259
- On PTX10008 devices, when the `NSR Enabled` and `FMBB` statements are configured and if SIB is Offline/ Online, the resiliencyd process generates core files. PR1766097
- FPCs experiences crashes and restarts whenever the network encounters either an MPLS LSP flap or a LAG flap. PR1767747
- Ambient-temperature value constantly changes after configuration. PR1767840
- The hwdre application restarts lead to non-functioning of GNMIC and memory components. PR1771597
- The Control Board and FPC restartes if the optics present in the first three ports of PTX10001-36MR devices draw 50W or more power. PR1775320
- Interface stay in link Down state when using third party optics. PR1776596
- The evo-aftmand-bt process crashes during an Routing Engine switchover. PR1776828
- Functionality provided by arp/ndp publish argument does not work on all Junos OS Evolved platforms. PR1776871
- On PTX100004, PTX100008, and PTX1000016 devices after GRES, the backup Routing Engine BITS left over alarms is still in the CM alarms. PR1777209
- LAG interfaces takes longer than usual to come up in a scaled scenario with ALB. PR1777759
- The rpd process generates core file when running the Telemetry for protocols from top of tree and while performing routing instance with add or delete operation. PR1778103
- Log message for DDoS violation information displays default time and incorrect date when its violation state is cleared by the `clear ddos-protection protocols states` statement. PR1778668
- License key is not installed after USB upgrade through the `set system license keys key` statement. PR1783509
- On PTX10016 devices, performing back to back SIB offline results in context deadline exceeded error. PR1784766

- IFBD lookup failure in DLU occurs and packets needs to be dropped rather than learned through control IFL in packetio. PR1785084
- The rpd crashes due to segment fault. PR1785884
- Difference in TOD between EEC and PTP FPGA is seen. PR1787869
- On PTX10000 devices with high multicast, route changes can trigger multicast traffic queue drops. PR1789679
- The pfestatsd process might fail to restart while running out of file descriptors. PR1790095
- COS mpls exp, dscp, and inet-precendence rewrite rules does not work on the Layer 2 SP and EP style interface for MPLS traffic. PR1793230
- Filter action decapsulation occurs in egress direction. PR1793356
- Port-mirroring issue gets observed while adding or deleting interface with port-mirror configuration. PR1796517
- Interface input drops and the Packet Forwrding Engine statistics information cell drop displays an incorrect large value with any configuration leading to IFD bounce. PR1796895
- PTX10001-36MR devices enters booting loop when a system reboot or software upgrade initiated reboot gets performed. PR1799275
- MPLS payload traffic coming over EVPN-MPLS tunnel gets dropped. PR1799760
- On PTX10001 devices, Minor Host 0 Voltage Threshold Crossed gets reported. PR1801330
- The `Host 0 Disk 1 Labelled incorrectly` alarm sometimes gets set and cleared in five seconds. PR1801436
- LACP goes down after adding native-vlan-id on the aggregated Ethernet interface with MACsec enabled on the child links. PR1802071
- Time-zone information gets changes to default UTC after upgrade gets done with restart-upgrade. PR1803511
- The `LICENSE_EXPIRED` syslog gets missed when license gets expired. PR1808956
- Fails to display SNMP object values on channelized interface. PR1790394

Infrastructure

- Tunnel interface configuration crossing routing instances might cause fibd to abort. PR1788995

Network Management and Monitoring

- lfmd fails to send notification about CRC error on the link. PR1769373

Routing Policy and Firewall Filters

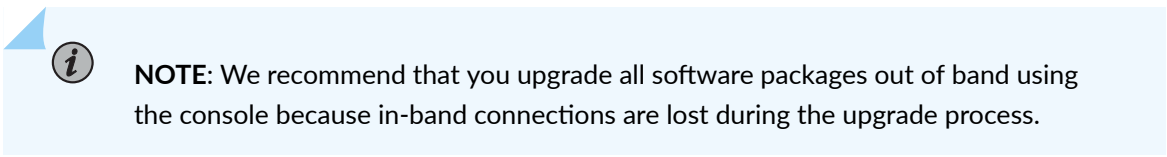
- The fwstatsd process crashes when openconfig-NI filter has the last term with only routing-instance action. PR1788695
- On PTX10004 devices, maximum configurable value of policer if-exceeding "bandwidth-limit" is 100Gbps. PR1798975

Upgrade Your Junos OS Evolved Software

Products impacted: ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016.

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

> **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.

- Visit Juniper Support Portal: Case Management, Product Support & More)
- 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

09 January 2026—Revision 15, Junos OS Evolved Release 24.2R1

23 September 2025—Revision 14, Junos OS Evolved Release 24.2R1

29 August 2025—Revision 13, Junos OS Evolved Release 24.2R1

26 June 2025—Revision 12, Junos OS Evolved Release 24.2R1

18 April 2025—Revision 11, Junos OS Evolved Release 24.2R1

28 February 2025—Revision 10, Junos OS Evolved Release 24.2R1

7 February 2025—Revision 9, Junos OS Evolved Release 24.2R1

4 February 2025—Revision 8, Junos OS Evolved Release 24.2R1

22 January 2025—Revision 7, Junos OS Evolved Release 24.2R1

23 December 2024—Revision 6, Junos OS Evolved Release 24.2R1

4 November 2024—Revision 5, Junos OS Evolved Release 24.2R1

24 October 2024—Revision 4, Junos OS Evolved Release 24.2R1

16 October 2024—Revision 3, Junos OS Evolved Release 24.2R1

28 August 2024—Revision 2, Junos OS Evolved Release 24.2R1

19 July 2024—Revision 1, Junos OS Evolved Release 24.2R1