Release Notes

Published
2025-05-26

Junos OS Evolved Release 24.2R2

Introduction

Use these release notes to find new and updated features, software limitations, and open issues for Junos OS Evolved Release 24.2R2.

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 24.2R2 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 24.2R2, 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.

Precision Time Protocol (PTP)

- **Assisted partial timing support (APTS) over Precision Time Protocol (ACX7024)**—Assisted partial timing support (APTS) is a Global Navigation Satellite System (GNSS) backed by Precision Time Protocol (PTP), which delivers accurate timing and synchronization in mobile backhaul networks. ACX7024 supports APTS.

  [See Assisted Partial Timing Support on Routing Platforms.]

- **Support for configurable hold over time interval (ACX7024)**—In an APTS setup when both GNSS and the PTP timing reference are lost or inactive, then the internal clock oscillator can provide synchronization. This functionality is enabled by default with a duration of 240 minutes. To configure this functionality, set the required duration in the newly introduced `set protocols ptp holdover-in-spec-duration` command on ACX7024.

  [See ptp.]

- [See G.8275.1 Telecom Profile, Guidelines for Configuring PTP over Ethernet, and Hybrid Mode.]

Routing Policy and Firewall Filters

-

- 

  NOTE: EVPN-MPLS configurations also support flood policers.

  [See **Policer Support for Aggregated Ethernet Interfaces Overview**.]

- **Support for profile categories (ACX7100-32C, ACX7100-48L, ACX7509, and ACX7024)**—Profile categories are a way to distinguish firewall filters based on the direction and interface type. The profile categories are namely, `ingress-inet6-user-acl`, `ingress-inet6-lo0-acl`, and `egress-inet6-user-acl`.

  [See Overview of Firewall Filter Profiles on ACX Series Routers (Junos OS Evolved).]

Additional Features

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

- [See EVPN Proxy ARP and ARP Suppression, and Proxy NDP and NDP Suppression.]
- [See **Configuring Q-in-Q Tunneling and Q-in-Q Tunneling and VLAN Translation**.]

What's Changed

IN THIS SECTION

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

EVPN

- **EVPN system log messages for CCC interface up and down events**—Devices will now log EVPN and EVPN-VPWS interface up and down event messages for interfaces configured with circuit cross-connect (CCC) encapsulation types. You can look for error messages with message types EVPN_INTF_CCC_DOWN and EVPN_INTF_CCC_UP in the device system log file `/var/log/syslog`).

General Routing

- **Change to the commit process**—In prior Junos OS and 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.
- On Junos OS Evolved, password authentication for SCP based configuration archival is supported.
- In a firewall filter configured with a port-mirror-instance or port-mirror action, if l2-mirror action is also configured, then port-mirroring instance family should be any. In the absence of the l2-mirror action, port-mirroring instance family should be the firewall filter family.

Routing Protocols

- **Update to IGMP snooping membership command options**—The `instance` option is now visible when issuing the `show igmp snooping membership ?` command. Earlier, the `instance` option was available but not visible when `?` was issued to view all possible completions for the `show igmp snooping membership` command.

  [See show igmp snooping membership.]

- **MLD snooping proxy and l2-querier source-address (ACX7024, ACX7100-32C, PTX10001-36MR, QFX5120-32C, and QFX5130-32CD)**—The `source-address` configured for `proxy` and `l2-querier` under the `mld-snooping` hierarchy should be an IPv6 link-local address in the range of fe80::/64. The CLI help text has been updated to "Source IPv6 link local address to use for proxy/L2 querier". In earlier releases, the CLI help text read, "Source IP address to use for proxy/L2 querier."

  [See source-address.]

User Interface and Configuration

- **Access privileges for request support information command (ACX Series, PTX Series, QFX Series)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance`, `view`, and `view-configuration` can execute request support information command.

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

- 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

- On all Junos OS Evolved platforms, port LED goes unlit or off instead of amber or on when port is disabled.PR1690655
- ACX7509 systems have the ability to do automatic fault-based switchovers when traffic impacting faults are seen on primary Routing Engine or primary FEB. This ability needs to be disabled if the backup Routing Engine because of this PR. The workaround is to disable automatic fault-based switchovers also as follows: `set chassis redundancy failover disable`. PR1713851
- When ingress policer is configured, to drop ingress traffic, on an interface with upMep the CFM packets generated from the upMep is also dropped due to the policer. This leads to CFM session going down. PR1754938
- When DHCP trace options are enabled, there is a possibility that jdhcpd could generate a core file. In general, traceoptions must be enabled only for debugging. They must be disabled once debuffing is done.PR1771121
- This is day-1 issue of Juniper Networks servo. It exists on all ACX Series platforms where Juniper Networks servo runs. Once the asymmetry configured at secondary port, the error propagated to the down stream eventually causes the performance issue of spike.PR1793926
- When multicast packets are transiting ACX7100 devices through VXLAN VTEP or core file interface without multicast configurations, errors are seen. Suggested to use DDOS configurations provide with workaround. PR1796501
- On Junos Evolved ACX7348 performing functions such as GRES (Graceful Routing Engine Switchover) or a `request node reboot re` is graceful, that is there is no traffic impact. PR1817121
- On ACX7348, ACX7332, or ACX7024 platforms, The SDK (Software Development Kits) initialization fails resulting in evo-pfemand application core file. This typically happens after evo-pfemand application restart or after a Routing Engine switchover.PR1842389
- On ACX7509 Junos Evolved platforms, picd crash is seen with protocol flaps in case of HA (High Availability) during RE (Routing Engine) switchover, caused due to incomplete initialisation. PR1863708

Infrastructure

- On all Junos Evolved ACX platforms, modifying an ECMP route triggers the deletion of the old Next Hop route, which can temporarily disrupt traffic flow until the new route is fully established.PR1820482

Routing Policy and Firewall Filters

- When using input-list we do not report the policer statistics correctly for Routing Engine filters. This is done correctly for interface-specific filter for the same.PR1844737

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. It's been a recommended practice to configure a global AS number in the field.PR1783375

Subscriber Access Management

- On Junos Evolved platforms, after device has finished booting up with Zero Touch Provisioning (ZTP), authd process crashes and generates a core file.PR1812697

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

- [ACX7100] PSM input under voltage failure is displayed in `show chassis hardware` but PSM status is OK. PR1757471
- CRC errors observed with SFT-T (740-013111 and 740-027085) optics. PR1771671
- Multihop BFD packets always uses the network-control egress queue. PR1776127
- LT interface does not work when Routing Engine switchover is triggered or primary Routing Engine evo-pfemand app process restarts. PR1778137
- PTP remains in ACQUIRING state. PR1783545
- L3 vlan tagged packets dropped and tagged as egress marking error in the egress L3VPN interface over tunnels (IP, SRv6, Dynamic etc). PR1789481
- Error messages populate **getQosRewriteHwMapIdFromIflIndex** and interface physical interface queue statistics traffic goes to the wrong queue. PR1793256
- Junos OS Evolved ACX Series platform does not respond to ICMP or SSH destined to VRF interface without vrf-table-label. PR1798925
- Traffic drop observed for next-hop. PR1800208
- Junos OS Evolved ACX platforms is powered down randomly due to incorrect read of temperature sensor. PR1801225
- Parameters on xSTP interface are not as expected after switchover. PR1801786
- The MPLS tunnel traffic arriving at the ingress interface drops on ACX7000 platforms when storm control is enabled. PR1802525
- [ACX7000] IPSEC-AH configuration enabled OSPF or OSPF3 session does not work. PR1803437
- Traffic loss is observed when renaming the VPLS routing-instance leading to MAC learning issues over LSI. PR1805586
- Traffic loss is seen due to stale route after running a test script on Junos Evolved platforms. PR1807906
- 1 second time offset can be seen on ACX7024 in the T-GM setup. PR1808134
- Usage alerts about re0:tempfs, mounted on /run/user/#### being marked as full. PR1808552
- L2ald-agent core file and IRB logical interface stays Hardware-down after deletion of IRB (with virtual-gateway-address config), readding same virtual-gateway-address as IRB address and move back to IRB with same virtual-gateway-address. PR1808779

- Traffic drop is seen for the affected ECMP flows on Junos Evolved ACX platforms. PR1810357
- The timingd process crash is seen on ACX7332 and ACX7348 platforms with GNSS service enabled. PR1810561
- ACX7100-not able to have more than 256 single-hop BFD sessions. PR1812652
- Failed to create LT interface due to an error message. PR1813565
- OSPFv3 neighborship does not form when configured over an IRB interface when MLD snooping is enabled on the bridge domain where IRB is hosted. PR1816540
- On ACX7348 and ACX7332, Jack Out Jack In of FPC blocks MACsec traffic. PR1818810
- Negative values are seen for jnxOperatingUpTime SNMP MIB after ~248 days uptime. PR1819254
- Traffic drop seen with HQOS on VLAN interface in EVPN FXC scenario on Junos OS Evolved ACX Series. platforms PR1820024
- 100G LR4 optics does not come up after upgrade on Junos Evolved ACX7509 platform. PR1821275
- Excessive logging in various log files is observed on Junos OS Evolved ACX Series platforms. PR1821807
- [Junos OS Evolved] DDoS message logs has a spelling mistake and need to be modified from **bandwith** to **bandwidth**. PR1822419
- MPLS payload ether-pseudowire configured along with any other MPLS payload type does not work as expected. PR1824219
- Object anomalies seen post deactivate or delete of PTP configurations. PR1833150
- Major FEB alarm due to broadsync unlock. PR1835268
- Picd and securityd process crashes during FPC or system restart. PR1836262
- On ACX Series Junos OS Evolved devices inline-sampling for sflow does not work with default route advertised through BGP. PR1836394
- Junos Evolved ACX7000 platforms might experience packet drops due to a delay in route update. PR1839055
- High CPU utilization observed on all Junos Evolved ACK7000 platforms.PR1841573
- Traffic is flooded for a prolonged time when mac-table-size is reduced. PR1845015
- Traffic statistics are missing for ipdemux lite subscribers for certain Junos Evolved ACX Series platforms PR1850651

- The evo-pfemand process crashes on ACX Series platforms without specific trigger. PR1854255

Class of Service (CoS)

- [Junos OS Evolved] cosd application might crash when the `interface-set` statement is configured under class-of-services hierarchy. PR1829632

Infrastructure

- The rpd process crashes when routing-instance type is changed from L2 to L3 or vice versa. PR1802000

Network Management and Monitoring

- There is no option for inband management through SNMPv3 on an interface configured with non-default routing instance. PR1814315
- The mib2d crash is observed on Junos OS Evolved platforms with duplicate SNMP request. PR1815524

Junos OS Evolved Release Notes for PTX Series

IN THIS SECTION

These release notes accompany Junos OS Evolved Release 24.2R2 for PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016, and PTX10002-36QDD 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 24.2R2, click the Group by Release link. You can collapse and expand the list as needed.

- PTX10001-36MR
- PTX10003
- PTX10004
- PTX10008

- PTX10016

The following sections highlight the key features in this release.

Hardware

- **PTX10002-36QDD router (PTX Series)**—The PTX10002-36QDD is a fixed-configuration router that features 36 high-density and cost-efficient 800-Gigabit Ethernet (800GbE) ports network ports in a 2-U form factor. With 28.8 terabits per second (Tbps) of throughput, the PTX10002-36QDD is optimally designed for peering, core routing, and infrastructure edge routing roles in cloud provider, service provider, and content provider networks.

  The router supports 2200-W or 3000-W high-voltage HVAC/HVDC and DC power supply units (PSUs) and front-to-back airflow.

  You can channelize the ports on the PTX10002-36QDD and increase the number of interfaces.

  To install the PTX10002-36QDD router and perform initial configuration, routine maintenance, and troubleshooting, see the PTX10002-36QDD Hardware Guide. See Feature Explorer for the complete list of features for any platform.

Table 1: PTX10002-36QDD Feature Support

Feature	Description
Chassis	• Support for the following chassis management functionalities: • The presence of two ASIC packages enables you to take a Flexible PIC Concentrator (FPC) offline or bring it online to restart the FPC without impacting the power to the FPC. • When you connect 3000-watt (W) power supply units (PSUs), the system operates in normal power mode. You can change the operating power mode from normal to power-optimized by using the `set chassis mode power-optimized` command. • The `show chassis fpc` command displays both **PFE** and **PFE-Instance** details. • On the router, when you run the `request chassis fpc` command, you must use `pfe`instead of `pfe-instance` to control the FPC operations. Also, when you run the `request chassis fpc` command, you must commit the command for both the Packet Forwarding Engines that are present. [See Power Mode Management on PTX10002-36QDD, chassis, request chassis fpc, and show chassis fpc.] • Support for resiliency features to manage fabric faults, including but not limited to: • Auto-heal functionality to recover the faulty link by fixing the errors automatically. • All Packet Forwarding Engines disabled when the number of fabric link errors exceeds four in the system. You can use the existing CLI commands for the fabric management. The following commands display new or different fields in their outputs: • `show chassis fabric fpcs` displays peer **FPC** and **PFE** details because the Packet Forwarding Engines are directly connected to each other.

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• `show chassis fabric topology` displays only physical link connectivity. [See Chassis-Level User Guide, show chassis fabric fpcs, and show chassis fabric topology.] • Optics EM policy support. We've extended the Junos Environment Monitoring (EM) policy to include optics temperature sensors for PTX10002-36QDD routers. It includes the following features: • The Optics EM policy incorporates periodically polled temperature readings of optical modules in the system to automatically manage the fan speed. • Junos OS Evolved automatically triggers optics shutdown for 100GbE, 400GbE, and 800GbE optics when the Fire Shutdown threshold is breached. Auto-recovery is not supported for optics disabled by the EM policy. To re-enable the optics, use the `request interface optics-reset` command or perform optics online insertion and removal (OIR). • EM policy is enabled by default on all 100GbE, 400GbE, and 800GbE optics that are Multi-source Agreements (MSA)-compliant and support diag EEPROM with temperature monitoring. This policy is not applicable for loopback optics and direct attach copper (DAC) cables. To disable EM policy or view temperature threshold values, use the following CLI commands: • `set chassis fpc` *`fpc_slot`* `pic` *`pic_slot`* `port` *`port_no`* `no-temperature-monitoring` explicitly disables the EM policy on specific WAN ports. • `show chassis temperature-thresholds` displays the optics temperature threshold values. • `show chassis environment` displays the optics temperature. [See chassis-adc-temperature-sensor.]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Routing Engine support. The fixed-configuration PTX10002-36QDD router supports an inbuilt Routing Engine represented by the model number `RE-JNP10002-36QDD` in the CLI. The router does not support: • A pluggable Routing Engine • GRES, as the router does not have a redundant Routing Engine • The following operational commands: • `request chassis routing-engine master acquire` • `request chassis routing-engine master release` [See show chassis hardware.] • Routing Engine resiliency. We've enabled Routing Engine resiliency for the faults related to CPU memory and DIMM. The Routing Engine supports fault-handling actions such as logging errors, raising alarms, sending SNMP traps, and providing indication about an error through the LEDs. [See show system errors active.] • Support for fabric platform resiliency includes resiliency functionality to manage hardware components such as the FPCs, PSUs, and fans. [See show chassis power detail, show chassis fpc, and show chassis fan.] • Packet Forwarding Engine resiliency. The software detects, reports, and takes action on Packet Forwarding Engine faults. Actions are taken based on the default configuration or user configuration available for the errors. [See show system errors active.]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
Class of service	• Support for class-of-service (CoS) features, including classifiers (behavior aggregate (BA), fixed, and multifield (MF)), rewrite rules, forwarding classes, loss priorities, transmission scheduling, rate control, and drop profiles. [See CoS Features and Limitations on PTX Series Routers.] • Support for priority-based flow control (PFC) watchdog, which detects and mitigates PFC pause storms received for PFC-enabled queues. We've added the `jnxCosWatchdogTxQueueTable` table to the SNMP class-of-service (CoS) MIB to show statistics for transmitting PFC queues related to the PFC watchdog. Table entries are indicated by `jnxCosWatchdogTxQueueEntry` and contain the following objects: • `jnxCosWatchdogIfIndex`—The index of an interface on which PFC and PFC watchdog are enabled. • `jnxCosWatchdogTxQueueId`—The ID of the queue of the PFC-enabled interface. • `jnxCosWatchdogTxQueueRecoveredCount`—The number of times a queue recovered after a PFC pause storm. • `jnxCosWatchdogTotalPktDrop`—The total number of packets dropped due to PFC pause storm mitigation since the device was started. • `jnxCosWatchdogLastPktDrop`—The number of packets dropped due to the last PFC pause storm. [See SNMP MIBs and Traps Supported by Junos OS and Junos OS Evolved and PFC Watchdog.] • Support for importing existing classifier and rewrite rules to form new rules. • Support for priority-based flow control (PFC) at Layer 3 for untagged traffic and explicit congestion notification (ECN).

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	[See Understanding PFC Using DSCP at Layer 3 for Untagged Traffic and CoS Explicit Congestion Notification.] • Queue-depth monitoring support for virtual output queues. Virtual output queue (VOQ) queue-depth monitoring, or latency monitoring, measures peak queue occupancy of a VOQ. Junos OS Evolved supports VOQ queue-depth monitoring to report peak queue length for a given physical interface for each Packet Forwarding Engine. [See VOQ Queue-depth Monitoring.] • Support for export of physical interface queue statistics to an outside collector. Use UDP (native) streaming, remote procedure call (gRPC) services, or gRPC network management interface (gNMI) services by using the sensor **/junos/system/linecard/interface/queue/**. Each physical interface has eight queues. The following counters are exported as part of this sensor for all configured physical interfaces: • Transmitted packets and transmitted bytes • Red drop packets and bytes • Tail drop packets and bytes This feature includes zero suppression support. It does not include support for summed-up counters on aggregated Ethernet (ae) interfaces. [See sensor (Junos Telemetry Interface) and Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).] • Hierarchical CoS support. The router supports up to four levels of scheduling on an interface (physical interfaces, logical interface sets, logical interfaces, and queues). The router does not support hierarchical CoS on integrated routing and bridging (IRB) or aggregated Ethernet interfaces. Also, hierarchical CoS schedulers should not include buffer or drop profile configurations.

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	To enable hierarchical scheduling, set `hierarchical-scheduler` at the [`edit interfaces` *`interface-name`*] hierarchy level. [See Hierarchical Class of Service in ACX Series Routers.] • Support for classification override configured under a forwarding policy. [See CoS Features and Limitations on PTX Series Routers and Overriding the Input Classification.]
Dynamic Host Configuration Protocol	• DHCPv4 relay agent and DHCPv6 relay agent are supported. The router supports the following DHCP features: • DHCP Relay: Layer 3 (L3) interfaces • DHCP Relay: Option 82 for Layer 2 VLANs • DHCP Relay: Option 82 for L3 interfaces • Extended DHCP relay agent • Virtual router-aware DHCP (VR-aware DHCP) [See Extended DHCP Relay Agent Overview.]
Hardware	• 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. [See Hardware Compatibility Tool .]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
High availability and resiliency	• BFD support, including: • Distributed BFD and BFD-triggered local repair (BFD authentication is not supported.) • Independent micro-BFD sessions enabled on a per-member link basis for a LAG bundle • Inline BFD [See Understanding BFD .] • Support for IP-over-IP encapsulation to facilitate IP overlay construction over an IP transport network. An IP network contains edge devices and core devices. To achieve higher scale and reliability among these devices, use an overlay encapsulation to logically isolate the core network from the external network that the edge devices interact with. Static configuration or a BGP protocol configuration is used to distribute routes and signal dynamic tunnels. The dynamic-tunnels configuration creates IP-over-IP encapsulation-only tunnels in the Packet Forwarding Engine. The router does not support the following features: • Dynamic tunnel de-encapsulation operation • Next-hop-based statistics for dynamic tunnels • IP fragmentation at tunnel start point and path MTU discovery for IPv4/IPv6 [See Next-Hop-Based Dynamic Tunneling Using IP-Over-IP Encapsulation .] • Support for VRRP. The following features are not supported for VRRP on Junos OS Evolved: • ISSU

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Proxy ARP • MC-LAG • Distribution support on aggregated Ethernet interfaces • IRB • Inline delegation [See Understanding VRRP .]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
Interfaces	• Interface support. The PTX10002-36QDD supports multiple port speeds and various channels under each port. The router supports a maximum port speed of 400 Gbps in low power mode. In standard power mode, it supports a port speed of 800 Gbps, If a port speed is configured (or a port speed is determined by default) without configuring `number-of-sub-ports` (at the [`edit interfaces` *`interface-name`*] hierarchy level), the port operates in nonchannelized mode. [See Port Speed on PTX Routers.] • 400G-ZR and 400G-ZR+ support enhancements. We support 400G-ZR and 400G-ZR+ optics enhancements on the PTX10002-36QDD. The enhancements include application selection and configuration of target output power. You can view the advertised applications and switch between the applications. [See Features of 400ZR and 400G OpenZR+.] • Support for performance monitoring and TCA. We support performance monitoring for the PTX10002-36QDD optical transceiver modules. The current and historical performance monitoring metrics are accumulated into 15-minute and 1-day interval bins. You can view the metrics using the `show interfaces transport pm` command and manage optical transport links efficiently. [See show interfaces transport pm.] • Support for timing and synchronization. The PTX10002-36QDD supports Synchronous Ethernet compliant with the following ITU recommendations: • G.8262/G.8262.1—Specifies timing characteristics of Synchronous Ethernet equipment clock (EEC). • G.8264—Describes the Ethernet Synchronization Message Channel (ESMC). [See Synchronous Ethernet Overview.]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Support for load balancing under the `[edit forwarding-options enhanced-hash-key]` hierarchy. Load balancing includes: • GRE key inclusion for transit IPv4 and IPv6 traffic • IP Layer 3 fields • IP Layer 4 fields • IPv6 flow label inclusion • MPLS labels • MPLS port data • MPLS pseudowire traffic • Tunnel endpoint identifier (TEID) inclusion in GPRS tunneling protocol (GTP) packets • RSVP-TE load balancing in proportion to LSP bandwidth [See enhanced-hash-key.] • Support for 128-way equal-cost multipath (ECMP) routing for MPLS transit cases. The following features do not support 128-way ECMP: • Multicast • P2MP • MC-LAG • Weighted unilist • Consistent hashing • Link protection (MPLS)

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Adaptive load balancing • Class-based forwarding • Support for 256-way ECMP. You can configure a maximum of 256 equal-cost multipath (ECMP) next hops for external BGP (EBGP) peers. This feature increases the number of direct BGP peer connections, which improves latency and optimizes data flow. However, we support 128 ECMP next hops for MPLS routes. Note that we do not support consistent load balancing (consistent hashing) for IPv4 or IPv6 with this feature. [See Understanding BGP Multipath.] • Support for FTI-based encapsulation and de-encapsulation of IPv4 and IPv6 packets. You can configure IP-IP encapsulation and de-encapsulation on flexible tunnel interfaces (FTIs). The default mode is loopback encap mode. Use the `bypass-loopback` statement at the `[edit interfaces fti` *`number`* `unit` *`logical-unit-number`* `tunnel encapsulation ipip]` hierarchy level to change the mode to flattened encap mode to achieve line-rate performance. [See Tunnel and Encryption Services Interfaces User Guide for Routing Devices.] • Support for configuring UDP tunnel encapsulation on FTIs. You can configure encapsulation by using the `tunnel encapsulation udp source` *`address`* `destination` *`address`* statement at the `[edit interfaces fti unit` *`unit`*`]` hierarchy level. Keep in mind the following when configuring this feature: • Adding `tunnel-termination` makes the tunnel a de-encapsulation-only tunnel and encapsulation is disabled. • Specifying both the source and destination address is mandatory when you do not configure `tunnel-termination`. • Configuring a variable prefix mask on the source address is not allowed.

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	[See encapsulation (interfaces-fti).] • **GRE tunnel encapsulation using loopback-based interface.** You can configure GRE tunnel encapsulation on flexible tunnel interfaces (FTIs) using the loopback interface. Configure encapsulation by using the `tunnel encapsulation gre source` *`address`* `destination` *`address`* statement at the `[edit interfaces fti0 unit` *`unit`*`]` hierarchy level. [See encapsulation (interfaces-fti).] • Support for GRE tunnel de-encapsulation using FTIs. Flexible tunnel interfaces (FTIs) support GRE tunnel de-encapsulation. When you enable the `tunnel-termination` statement at the `[edit interfaces fti0 unit` *`unit-number`*`]` hierarchy level, tunnels are terminated on the WAN interface before any other actions—such as sampling, port mirroring, or filtering—are applied. [See Tunnel and Encryption Services Interfaces User Guide for Routing Devices.] • Support for configuring MPLS protocols over FTI tunnels, thereby transporting MPLS packets over IP networks that do not support MPLS. Generic routing encapsulation (GRE) and UDP tunnels support the 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 level. [See Flexible Tunnel Interfaces Overview.]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
Junos telemetry interface	• JTI support for Packet Forwarding Engine sensors for usage, network processing unit (NPU) memory, NPU utilization, and pipeline NPU and ASIC. Using the Junos telemetry interface (JTI), you can export statistics using remote procedure call (gRPC) services, gRPC Network Management Interface (gNMI) services, and UDP transport. Use these sensors: • `/junos/system/linecard/packet/usage/` • `/junos/system/linecard/npu/memory/` • `/junos/system/linecard/npu/utilization/` • `/components/component/integrated-circuit/state/` • `/components/component/integrated-circuit/pipeline-counters/` For pipeline sensors, the four packet and drop counter categories are `interface`, `lookup`, `queuing`, and `host interface`. [See Junos YANG Data Model Explorer.] • JTI support for platform sensors. Using the Junos telemetry interface (JTI), you can export platform-specific software and chassis component statistics using remote procedure call (gRPC) services, gRPC Network Management Interface (gNMI) services, and UDP transport. Use these sensors: • **/junos/system/cmerror/** • **/junos/system/linecard/** • **/components/components/** • **/system/alarms/** • **/state/interfaces/**

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• **/state/chassis/** [See Junos YANG Data Model Explorer.]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
Layer 2 features	• Support for flow-aware transport (FAT) for pseudowires labels on ingress routers, with parsing that includes all the payload fields in the hash calculation. These flow labels are supported: • L2circuit, LDP-signaled pseudowires • L2VPN, BGP-signaled pseudowires • L2VPN with FEC129 (BGP autodiscovery) [See flow-label-receive and flow-label-transmit.] • Support for VLAN tag manipulation: pop, push, and swap. [See Configuring an MPLS-Based VLAN CCC with Pop, Push, and Swap and Control Passthrough.] • Support for virtual circuit connection verification (VCCV) protocol, which transfers control packets from one provider edge (PE) router to another PE router by creating a separate channel in the pseudowires. The pseudowires set up signaling peers and use a control word to maintain proper sequencing of pseudowire packets over the packet-switched network. [See BFD Support for VCCV for Layer 2 VPNs, Layer 2 Circuits, and VPLS, Configuring BFD for VCCV for Layer 2 Circuits, MPLS Pseudowires Configurationshow ldp database, and show route instance.] • Support for inner VLAN transparency. We support the pop, push, swap, pop-pop, pop-swap, swap-push,push-push, and swap-swap operations on port-based and VLAN-based Metro Ethernet Forum (MEF) Layer 2 services. VLAN transparency refers to preserving inner VLANs in the packet that are not subject to manipulation and are not used for forwarding. Based on the scenarios, VLAN transparency works on up to four VLAN tags. [See Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services.] • Support for the following protocols:

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	1. LAG (aggregated Ethernet) 2. LACP 3. LLDP

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
Layer 3 features	• Support for the following Layer 3 forwarding features: • IPv4 • IPv6 • MPLS • LAG • ECMP • MTU checks • ICMP • OSPF • IS-IS • ARP • NDP • BGP • BFD • LACP • LDP • RSVP • LLDP • VRF-lite • TTL expiry • IP options

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• IP fragmentation • DDoS

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
MACsec	• MACsec support in static CAK mode on physical interfaces with dynamic power management. Media Access Control Security (MACsec) is an industry-standard security technology that provides secure communication for traffic on Ethernet links. This device supports MACsec in static connectivity association key (CAK) mode. This device supports MACsec on physical interfaces to enable you to secure your network using any of the following encryption types: • GCM-AES-128 • GCM-AES-256 • GCM-AES-XPN-128 • GCM-AES-XPN-256 This device supports the following MACsec features: • Configurable security association key (SAK) rekey period • MACsec Key Agreement (MKA) protocol fail-open mode • Preshared key (PSK) chains and hitless rollover • PSK password encryption using single password • Fallback PSK • Extended packet numbering (XPN) • Jumbo frames [See Understanding Media Access Control Security (MACsec).] • MACsec dynamic power management support. Use MACsec to secure your network with the knowledge that your device is working to optimize power usage. To save power, the device dynamically powers MACsec blocks on and off based on the MACsec configuration.You might experience minimal traffic loss during the power block transition. [See Understanding Media Access Control Security (MACsec).]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
MPLS	• Support for MPLS FRR. MPLS fast reroute (FRR) provides faster convergence time (less than 50 milliseconds) for RSVP tunnels. The Routing Engine creates backup paths, and the Packet Forwarding Engine installs the backup-path labels and next hops. [See Fast Reroute Overview.] • Support for MPLS features,including: • CLI support for monitoring MPLS label usage • Inline MPLS and IPv6 lookup for explicit null • 32,000 transit LSPs • Explicit null support for MPLS LSPs • MPLS label block configuration • MPLS over untagged Layer 3 interfaces • MPLS OAM: LSP ping • JTI: OCST: MPLS operational state streaming (v2.2.0) • 2000 ingress LSP support • 2000 egress LSP support • Entropy label support • MPLS: JTI: Junos telemetry interface MPLS self-ping and TE++ • LDP, including: • Configurable label withdraw delay • Egress policy

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Explicit null • Graceful restart signaling • IGP synchronization • Ingress policy • IPv6 for LDP transport session • Strict targeted hellos • Track IGP metric • Tunneling (LDP over RSVP) • RSVP++ • RSVP-TE, including: • Bypass LSP static configuration • Ingress LSP statistics in a file • RSVP-TE hitless-MBB with no artificial delays • 32,000 transit LSPs • Auto bandwidth • Class-based forwarding (CBF) with 16 classes • CBF with next-hop resolution • Convergence and scalability • Graceful restart signaling • JTI interface statistics and LSP event export • LSP next-hop policy

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• LSP self-ping • MPLS fast reroute (FRR) • MTU signaling • Optimize adaptive teardown • Node/link protection • Refresh reduction • Soft preemption • Shared Risk Link Group (SRLG) • Static LSPs with IPv4 next hop, IPv6 next hop, and IPv6 next hop with next-table support for bypass • Traffic engineering, including: • TE++: Dynamic ingress LSP splitting • Traffic engineering extensions (OSPF-TE and ISIS-TE) • Traffic engineering options: `bgp`, `bgp-igp`, `bgp-igp-both-ribs`, and `mpls-forwarding` [See MPLS Applications User Guide .] • Support for an increased scale of transit RSVP-TE–signaled MPLS label-switched paths (LSPs) that are enabled with link protection. • Enhanced scaling for the following MPLS features: • RSVP transit LSPs with link and node protection • RSVP ingress and egress LSPs with ultimate-hop popping (UHP) and penultimate-hop popping (PHP) • LDP-over-RSVP LSPs

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Packet Forwarding Engine statistics • Fast reroute (FRR) and make before break (MBB) • Weighted ECMP • Ping and traceroute • Clone route • Transit statistics [See MPLS Applications User Guide .] • Support for RSVP-based and LDP-based point-to-multipoint (P2MP) LSPs with graceful restart. In addition, the router supports IP unicast traffic in a label-edge router (LER) role and both IP unicast and multicast traffic in a label-switching router (LSR) role. [See Point-to-Multipoint LSPs Overview.] • Support for MPLS features P2MP ping and P2MP LSPs traceroute. MPLS ping and traceroute provide the mechanism to detect data-plane failure and isolate faults in the MPLS network. The traceroute or ping is initiated to validate LSP paths on P2MP. [See MPLS Applications User Guide .] • Optimized fast branch updates. We've refined the method of making fast-branch updates to a multicast replication tree. Now, any membership changes in the tree trigger fast make-before-break (FMBB) re-optimization of the tree and ensure that there is no traffic loss. [See Multicast Shortest-Path Tree.]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
Multicast	• MVPN BIER with MPLS encapsulation. Junos OS Evolved supports the Bit Index Explicit Replication (BIER) architecture to simplify control and forwarding planes by eliminating the need for multicast trees and per-flow states. With BGP-MVPN as an overlay, you can configure BIER-enabled provider tunnels for multicast VPNs. [See BIER Overview and bier.] • IS-IS as routing underlay for BIER. Junos OS Evolved supports the advertisement of BIER information of one or more BIER subdomains using IS-IS as the IGP underlay. Key BIER information such as BFR IDs and BFR prefixes in each subdomain are flooded through the IS-IS domain to generate the BIER forwarding table. [See IS-IS Extension for BIER and bier-sub-domain (Protocols IS-IS).] • IPv4 and IPv6 multicast support including MSDP, support for PIM-SM as the first-hop router (FHR) or last-hop router (LHR), and support for anycast, static, or local rendezvous point (RP). • Support for multicast-only fast reroute (MoFRR) for both IPv4 and IPv6 traffic flows. MoFRR minimizes multicast packet loss in PIM domains when there are link failures. MoFRR is supported for PIM sparse mode (SM) and source-specific multicast (SSM) modes only. Support does not extend to Multipoint LDP-based MoFRR. [See **Understanding Multicast-Only Fast Reroute**.] • Support for bidirectional Protocol Independent Multicast (PIM) for multicast traffic. [See **pim-snooping**.]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
Routing policy and firewall filters	• Support added to hierarchical policers for applying user-selectable bandwidth for premium and non-premium traffic. Use the firewall filter action `policer-charge` to subtract available bandwidth credits and make bandwidth available to the aggregate policer. • Firewall output filtering support using Fast Lookup Filter (FFT) block for line-rate performance of up to 2 billion PPS. The `fast-lookup-filter` statement from the CLI filter configuration prioritizes output filtering (but not input filtering) on the FFT block. FFT enables support for 128 unique output filters across IPv4, IPv6, or MPLS families. [See fast-lookup-filter (PTX).] • SNMP MIB support for the `jnxFirewallCounterTable` object. Junos OS Evolved SNMP extends support for the `jnxFirewallCounterTable` and its objects: • `jnxFirewallCounterEntry` • `jnxFWCounterPacketCount` • `jnxFWCounterByteCount` • `jnxFWCounterDisplayFilterName` • `jnxFWCounterDisplayName` • `jnxFWCounterDisplayType` [See SNMP MIB Explorer.] • Firewall filter support. IPv4 and IPv6 firewall filters provide rules that define whether to permit, deny, or forward packets that are transiting an interface on the router from a source address to a destination address. [See Firewall Filter Match Conditions and Actions (PTX Series Routers).] • Support for filter-based forwarding.

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	[See Example: Configuring Filter-Based Forwarding to a Specific Outgoing Interface or Destination IP Address.] • Support for SDN-based networks to configure certain router interfaces to pass traffic toward an SDN controller. Use firewall filters to match and redirect packets defined at the `[edit services inline-monitoring instance]` hierarchy level. Supported match criteria includes IPv4, IPv6, and family `any` (destination), VLAN ID, and certain traceroute redirect packets. [See controller.] • Support for firewall filters on discard interfaces. You can apply firewall filters on a discard interface. The action specified by the filter (log or count) is executed before the traffic is discarded. Firewall filters are supported only for IPv4 and IPv6 traffic in the egress direction of the interface. [See Configuring Firewall Filters.] • Support for firewall features, including: • Forwarding IPv4 and IPv6 • Firewall filter • Load balancing • MPLS fast reroute • Host path • Egress peer engineering [See Firewall Filter Match Conditions and Actions (PTX Series Routers).] • Support for input-chain and output-chain CLI filters. Use multiple levels of CLI filters. The filter chain helps in logically grouping filters with a specific pattern of rules, instead of evaluating all the filter terms in one filter and deciding at the filter's last term. The feature provides you flexibility in

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	modeling the filter as and when it is applicable in the solution. You can configure up to eight filters in both input chains and output chains. [See Example: Using Firewall Filter Chains, output-chain, and input-chain.] • Support for nested filters, which enable you to reference a common firewall filter by attaching it to multiple firewall policies (a filter being one or more match conditions and corresponding actions). You can bind nested filters to the following interface types: • `inet`—Both input and output directions • `inet6`—Both input and output directions • `mpls`—Input direction only You can also bind the filters to routing instances, and in the input direction, in the output direction, or in both directions. [See Guidelines for Nesting References to Multiple Firewall Filters and Example: Nesting References to Multiple Firewall Filters.] • Support for matching `ip-options` in IPv4 packet headers. Use the `ip-options any` match condition to match fields in the IPv4 header and create firewall filter rules to handle the matched packets. Specifying `ip-options` provides a finer level of control, so for example, you can create a rule to drop any IPv4 packets that do not include at least one IP option in the header. Configure the match condition at the `[edit firewall family inet filter` *`name`* `term` *`name`* `from ip-options any]` hierarchy level. [See Firewall Filter Match Conditions for IPv4 Traffic .] • Support for labeling interfaces with specified group IDs from 1 through 255 and matching the interface-group ID on the firewall filter. The filter recognizes which interface the packet comes from and performs actions only specified for a certain interface group.

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	[See Understanding BGP Flow Routes for Traffic Filtering .] • Firewall filter support for bitwise logical operations for TCP flag match. [See Firewall Filter Match Conditions Based on Bit-Field Values .] • MPLS filter payload match. IPv4 and IPv6 payload fields match conditions are available for MPLS traffic. Additionally, the following match conditions are available: • MPLS header EXP match conditions for MPLS traffic—`exp0`, `exp1`, `exp0-except`, `exp1-except`. Existing match conditions `exp` and `exp-except` will be deprecated. • MPLS header Label match conditions for MPLS traffic—`label0`, `label1`, `label0-except`, `label1-except`. Existing match conditions `label` and `label-except` will be deprecated. • MPLS header TTL match conditions for MPLS traffic—`ttl0`, `ttl1`, `ttl0-except`, `ttl1-except`. Existing match conditions `ttl` and `ttl-except` will be deprecated. • MPLS header Bottom of Stack match conditions for MPLS traffic—`bottom-of-stack0` and `bottom-of-stack1` [See Firewall Filter Match Conditions for MPLS Traffic .] • Unicast RPF support for both IPv4 and IPv6 traffic flows. [See Configuring Unicast RPF Loose Mode.] • Enhanced scaling for DoS and protection offers loose mode unicast RPF on IPv4 and IPv6. [See Configuring Unicast RPF Loose Mode.] • Support for DCU and SCU accounting. Source class usage (SCU) accounting provides a breakdown of output interface traffic statistics that originates from specific prefixes. Destination class usage (DCU) accounting provides a

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	breakdown of input interface traffic statistics that is destined for specific prefixes. [See Understanding Source Class Usage and Destination Class Usage Options.] • Class-based firewall filters. You can apply firewall filters actions such as `drop`, `reject`, `sample`, and `police` on packets classified by destination class usage (DCU) and source class usage (SCU) accounting. You can use this feature, for example, as part of a design to provide distributed denial-of-service (DDoS) protection to specific customers. [See Configure the Filter Profile.] • Support for forwarding class and packet loss priority (PLP) as policer actions. You can use forwarding class (FC), and both FC and PLP together, as policer actions in policer policy configurations. This includes both ingress and egress directions. • Support for two-color Layer 3 interface policers (ingress and egress). [See Basic Two-Rate Three-Color Policers.] • Support for packet-rate policers. You can use a count of packets as the threshold for traffic policers. Per-packet policers can better mitigate low-and-slow types of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. You can apply packet-level policers in the ingress or egress interface direction. These policers support both two-color and three-color policers. The following families are supported: `inet`, `inet6`, `mpls`, and `ethernet-switching` . Configure per-packet policer rates using the `pps-limit` (packets per second) and `packet-burst-size-limit` (packets) configuration statements at the `[edit firewall policer` *`policer-name`*`]` hierarchy level. [See Packets-Per-Second (pps)-Based Policer Overview and pps-limit (Policer).]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Shared-bandwidth and percentage policer. Use the shared-bandwidth policer for instances where policers are attached to aggregated Ethernet interface bundles with child legs spanning different Packet Forwarding Engine or Flexible Port Concentrator (FPC) instances. The bandwidth policers program the policer token bucket with weighted bandwidth or burst (depending on the number of child legs per Packet Forwarding Engine). The percentage policer feature enables you to configure the bandwidth policer relative to the physical-interface speed where you configure the class-of-service (CoS) shaping rate. After the configuration, the egress policer can then use this base CoS shaping rate instead of the physical-interface speed. [See Configure the Filter Profile.] • Two-color and three-color traffic policers for input and output traffic. The supported actions are `discard`, `forwarding-class`, and `loss-priority` (`high` and `low`). You can attach policers to logical interfaces and the protocol families `mpls`, `inet`, and `inet6`. [See Basic Two-Rate Three-Color Policers.] • Filter-based GRE encapsulation and de-encapsulation and filter-based MPLS-in-UDP de-encapsulation. We've enabled the following encapsulation and de-encapsulation workflow: **1.** An incoming packet matches a filter term with an encapsulate action. The packet is encapsulated in an IP +GRE header and is forwarded to the endpoint's destination. `set firewall tunnel-end-point` *`tunnel-name`* `ipv4|ipv6 source-address` *`address`* `set firewall tunnel-end-point` *`tunnel-name`* `ipv4|ipv6 destination-address` *`address`* `set firewall tunnel-end-point` *`tunnel-name`* `gre` `set firewall family inet|inet6 filter` *`name`* `term` *`name`* `from source-address` *`address`*

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	`` set firewall family inet|inet6 filter name term name then encapsulate tunnel-name set firewall family inet|inet6 filter name term last then accept set interfaces interface-name unit number family inet|inet6 filter input set interfaces interface-name unit number family inet|inet6 address address # This source address differs from the one for the tunnel endpoint. ``` 2. At the destination, the packet matches a filter term with a de-encapsulate action. The GRE header or MPLS-in-UDP header is stripped from the packet. The inner packet is routed to its destination. ``` set firewall family inet|inet6 filter name term name from source-address address set firewall family inet|inet6 filter name term name from protocol gre set firewall family inet|inet6 filter name term name then decapsulate gre # Optionally de-encapsulate mpls-in-udp. set firewall family inet|inet6 filter name term last then accept set interfaces interface-name unit number family inet|inet6 filter input filter-name set interfaces interface-name unit number family inet|inet6 address address # This is the destination address. ``` [See Components of Filter-Based Tunneling Across IPv4 Networks and tunnel-end-point.] • Support for tunnel de-encapsulation using firewall filters for GRE and UDP tunnels. [See Configuring a Filter to De-Encapsulate GRE Traffic and decapsulate (Firewall Filter).]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
Routing protocols	• BGP flow specification. BGP can carry flow-specification network layer reachability information (NLRI) messages on PTX10002-36QDD devices with 14.4 Tbps line cards. Propagating firewall filter information as part of BGP enables you to propagate firewall filters against denial-of-service (DOS) attacks dynamically across autonomous systems. The following match conditions are not supported: • ICMP codes alone [`inet/inet6`] • Source/destination prefix with offset for `inet6` • Flow label for `inet6` fragment [for `inet6`] Junos OS Evolved running on this router doesn't support the traffic marking action. To configure flow routes statically, configure the match conditions and actions at the `[edit routing-options]` hierarchy level. • Forwarding IPv6 transit statistics. [See BGP User Guide.]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
Network management and monitoring	• Local port mirroring support. You can use port mirroring to copy packets entering or exiting a port or entering a VLAN and to send the copies to a local interface for local monitoring. The following features are included: • Interface filter on ingress and egress • Forwarding table filter (FTF) on ingress • Families `inet` and `inet6` • Aggregated Ethernet interfaces at both ingress and egress Use the following CLI hierarchies to configure port mirroring: • `[edit interfaces]` • `[edit forwarding-options port-mirroring]` • `[edit firewall filter]` You can configure family `inet` and family `inet6` in the `[edit interfaces]` and the `[edit forwarding-options port-mirroring]` hierarchies for this feature. This feature applies to global port mirroring only. [See Understanding Port Mirroring and Analyzers.] • Remote port mirroring with ToS or DSCP settings. You can send sampled copies of incoming packets to remotely connected network management software. You send the packets using GRE, which is supported by flexible tunnel interfaces (FTIs). You can set ToS and DSCP values to provide necessary priorities in the network for these packets. You can also apply policing to sampled packets that are leaving the FTI. Configure the settings you need in the `[edit forwarding-options port-mirroring instance` *`instance-name`* `output]` hierarchy. [See instance (Port Mirroring).]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Support for additional family `any` in port mirroring You can configure family `any` (as well as the earlier family options, `inet`, and `inet6`) for local port mirroring and remote port mirroring. You can use the family `any` configuration option to process the families `any`, `ccc`, `ethernet-switching`, or `mpls`. **NOTE**: You use the family `any` configuration option to process all four families. Use [`edit forwarding-options port-mirroring`] for local port mirroring or [`edit forwarding-options port-mirroring instance` *`instance-name`*] for remote port mirroring, with both configurations also requiring a firewall filter. The following configuration statements are no longer part of the port mirroring configuration on PTX Series devices: • `next-hop` for family `any` • family `vpls` • `no-filter-check` • `hosted-service` • `server-profile` [See port-mirroring.] • Support for EVPN-VXLAN filtering and port mirroring based on VNI match conditions. You can construct a firewall filter to filter EVPN-VXLAN traffic by using the VXLAN network identifier (VNI) values in the match condition on ingress and egress interfaces. This feature supports redirecting traffic to a global port-mirroring instance. To filter traffic based on the VNI, use the following commands: `set firewall filter` *`filter-name`* `term` *`term-name`* `from vxlan vni` *`vni-value`*

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	`set firewall filter` *`filter-name`* `term` *`term-name`* `from vxlan vni-except` *`vni-value`* *`vni-value`* can be a numeric value or range of numeric values. [See Firewall Filter Match Conditions and Actions (PTX Series Routers).] • Support for the sFlow technology, which is a monitoring technology for high-speed switched or routed networks. The sFlow monitoring technology randomly samples network packets and sends the samples to a monitoring station. [See sFlow Monitoring Technology.] • sFlow technology support for MPLS interfaces to sample and report MPLS traffic on the routers. [See sFlow Technology Overview.] • Ingress and egress sFlow functionalities for transit nodes are supported for IPv4-in-IPv4, IPv6-in-IPv4, and regular IPv4/IPv6 traffic. In transit-only devices, the IP-in-IP encapsulated packet can transit through the device without any change or might get de-encapsulated and forwarded or de-encapsulated and encapsulated and forwarded based on the next-hop configuration. Additionally, the packet might traverse through multiple VRF instances while getting forwarded. The router supports ingress and egress sFlow for all those variations. [See sFlow Monitoring Technology.] • sFlow technology support for exporting extended IPv4 and IPv6 tunnel egress structure. sFlow technology supports the export of the Extended Tunnel Egress Structure fields for traffic entering IPv4 or IPv6 GRE tunnels. These additional attributes provide information about the GRE tunnel into which a packet entering the device will get encapsulated. The GRE tunnel could be IPv4 or IPv6. The feature is supported only when sFlow is enabled in the ingress direction wherein firewall-based GRE happens on IPv4 or IPv6 packets.

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	The device supports the feature for the following traffic scenarios when ingress sFlow sampling is enabled: • Incoming IPv4 traffic that undergoes IPv4 GRE • Incoming IPv6 traffic that undergoes IPv4 GRE • Incoming IPv4 traffic that undergoes IPv6 GRE • Incoming IPv6 traffic that undergoes IPv6 GRE [See sFlow Monitoring Technology.] • Sample size support in sFlow. You can configure the sFlow sample size of the raw packet header to be exported as part of the sFlow record to the collector. The configurable range of sample size is from 128 bytes through 512 bytes. [See sFlow Monitoring Technology.] • Support for passive monitoring, including support for passive monitoring on MPLS-encapsulated packets. You can configure passive monitoring on any interface on the PTX Series routers, and you can use this feature to monitor MPLS-encapsulated packets. After you enable passive monitoring, the router accepts and monitors traffic on the interface and forwards those packets to monitoring tools such as IDS servers and packet analyzers, or to other devices such as other routers or end-node hosts. [See Passive Monitoring and passive-monitor-mode.] • Support for link fault management (LFM). We support IEEE 802.3ah OAM LFM to monitor point-to-point Ethernet links that are connected either directly or through Ethernet repeaters. The following LFM features are supported: • Link discovery with active and passive modes • Detect-LOC • Remote loopback

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Loopback tracking • Action profile • GRES and non-graceful Routing Engine switchover [See Introduction to OAM Link Fault Management (LFM).]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
Segment routing	• Segment routing support. You can configure the following Source Packet Routing in Networking (SPRING) or segment routing features on the router: • MPLS (segment routing using IS-IS): • Ping and traceroute for single IS-IS node or prefix segment • BGP Link State (BGP-LS): • Segment routing extensions for IS-IS • Segment routing extensions for OSPF • BGP: • Binding segment identifier (SID) for segment routing–traffic engineering (SR-TE) • Binding SID for SR-TE [draft-previdi-idr-segment-routing-te-policy] • Programmable routing protocol process APIs for SR-TE policy provisioning • Static SR-TE policy with mandatory color specification • Static SR-TE policy without color specification • IS-IS: • Adjacency SID • Advertising maximum link bandwidth and administrative color without RSVP-TE configuration • Anycast and prefix SIDs • Configurable segment routing global block (SRGB)

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Node and link SIDs • Segment Routing Mapping Server (SRMS) and client • Topology Independent Loop-Free Alternate (TI-LFA): • Link and node protection for IPv4 addressing (not required for IPv6 prefixes) • Link and node protection for IPv4 addressing (required for IPv6 prefixes) • Protection for SRMS prefixes • OSPF: • Advertising maximum-link bandwidth and administrative color without RSVP-TE configuration • Anycast SID • Configurable SRGB • Inter-area support • Node and link SID • Prefix SID • Segment Routing Mapping Server (SRMS) and client • Static adjacency SID • TI-LFA: • Link and node protection • Protection for SRMS prefixes

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• MPLS ping and traceroute for single OSPF node or prefix segment • IGP adjacency SID hold time • Path Computation Element Protocol (PCEP) for segment routing LSPs • BGP IPv4 labeled-unicast resolution over: • BGP IPv4 SR-TE with IPv4 segment routing using IS-IS and OSPF • Non-colored IPv4 SR-TE with segment routing using IS-IS and OSPF • Static colored IPv4 SR-TE with segment routing using IS-IS and OSPF • BGP Layer 3 VPN over: • Colored SR-TE tunnels and IPv4 protocol next hops • Non-colored SR-TE tunnels and IPv4 protocol next hops • BGP-triggered dynamic SR-TE colored tunnels • Class-based forwarding and forwarding table policy LSP next-hop selection among non-colored SR-TE LSPs • First-hop label support for SID instead of an IP address • Path specification using router IP addresses (segment routing segment list path ERO support using IP address as next hop and loose mode) • SR-TE color mode: • 00—Route resolution fallback to IGP path • 01—Route resolution fallback to color only null routes

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Static LSPs with member-link next hops for aggregated Ethernet bundles (also known as adjacent SID per LAG bundle or aggregated Ethernet member link) [See Understanding Source Packet Routing in Networking (SPRING).] • Support for scaled-up static and BGP segment routing policies, where each policy contains eight segment routing paths with five labels per path without make-before-break (MBB). [See egress-chaining and fib-next-hop-split.] • SPRING statistics sensor support for JTI supports export of SPRING statistics to an outside collector by using remote procedure call (gRPC) services. The feature provides the segment-identifier (SID)-level and interface-level traffic counts for SPRING traffic. These statistics reflect the SPRING LSP utilization in the traffic engineering database, which aids in correctly rerouting the RSVP LSPs. To enable SPRING statistics, include the following statements on the client device: • For egress (per-interface egress), use `set protocols isis source-packet-routing sensor-based-stats per-interface-per-member-link egress` • For egress (per-SID egress), use `set protocols isis source-packet-routing sensor-based-stats per-sid egress` • For ingress (per-SID ingress), use `set protocols isis source-packet-routing sensor-based-stats per-sid ingress`. Use the following sensors to export statistics by means of gRPC services to an outside collector: • **/junos/services/segment-routing/interface/egress/usage/** for egress (per-interface egress) aggregate SPRING traffic.

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• **/junos/services/segment-routing/sid/usage/** for egress (per-SID egress) and ingress (per-SID ingress) aggregate SPRING traffic. [See source-packet-routing and Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface.] • BGP and statically configured SR-TE traffic statistics sensor support for JTI. [See source-packet-routing, Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface, and Understanding OpenConfig and gRPC on Junos Telemetry Interface.] • Support for segment routing over UDP. Configure the `udp-tunneling encapsulation` statements at the `[edit protocols isis source-packet-routing]` hierarchy level to enable SR-MPLS routers and IP-only routers to seamlessly coexist, by encapsulating SR-MPLS label stacks in IP/UDP encapsulation. This feature also supports: • Entropy in the UDP source port • Underlay and overlay ECMP at the start of the tunnel • Policy control to resolve dynamic tunnels SR-over-UDP supports tunnels without a loopback stream in the Packet Forwarding Engine, thereby reducing additional bandwidth consumption. [See Next-Hop-Based Dynamic Tunnels and source-packet-routing (Protocols IS-IS).] • SPRING : JTI : Ingress SR-TE statistics per binding SID and segment list (static, BGP, PCEP paths). Use this feature to provide route statistics for segment routing-traffic engineering (SR-TE) per label-switched path (LSP). Junos OS Evolved uses Junos telemetry interface (JTI) and gRPC services to provide the statistics. Supported resource paths (sensors) include:

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• **/junos/services/segment-routing/traffic-engineering/tunnel/lsp/ingress/usage/** • **/junos/services/segment-routing/traffic-engineering/tunnel/lsp/transit/usage/** [See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface, source-packet-routing, and show spring-traffic-engineering.] • SPRING statistics sensor support for JTI supports export of SPRING statistics to an outside collector by using remote procedure call (gRPC) services and gRPC Network Management Interface (gNMI) services. This feature provides interface-level and segment identifier (SID)-level ingress statistics. The feature also provides egress statistics for each child member at the physical interface level. To enable SPRING statistics, include the following statements on the client device: • For egress (per-child member at the physical interface level), use the `set protocols isis source-packet-routing sensor-based-stats per-interface-per-member-link egress` command. • For ingress (per-SID ingress and per-interface ingress), use the `set protocols isis source-packet-routing sensor-based-stats per-interface-per-member-link ingress` command. Use the following sensors to export statistics by means of gRPC or gNMI services to an outside collector: • **/network-instances/network-instance/mpls/signaling-protocols/segment-routing/interfaces/interface/state/in-octets/** for ingress (per-SID ingress and per-interface ingress) SPRING traffic. • **/network-instances/network-instance/mpls/signaling-protocols/segment-routing/interfaces/interface/state/**

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	out-octets/ for egress (per-child member at the physical-interface level) SPRING traffic. • **/network-instances/network-instance/mpls/signaling-protocols/segment-routing/interfaces/interface/state/out-pkts/** for egress (per-child member at the physical-interface level) SPRING traffic. [See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface and source-packet-routing.] • Support for segment-routing telemetry sensor enhancements. We support segment routing sensor enhancements for SID-level and interface-level traffic counts. These enhancements comply with the current supported sensors in the OpenConfig models **openconfig-segment-routing.yang** and **openconfig-mpls.yang**. • SR-TE colored policy RIB5 and SR-TE colored telemetry sensor support. We support JTI streaming and ON-CHANGE sensors that deliver operational state statistics for SR-TE colored policy RIB5 and SR-TE colored telemetry sensors. Statistics are delivered to an outside collector using gRPC or gNMI. The feature includes new OpenConfig resource paths for existing and new SR-TE policy (tunnel) and SR-TE per-LSP colored statistics. [See Telemetry Sensor Explorer.] • Support for SRv6 network programming in IS-IS. Use this feature to configure segment routing in a core IPv6 network without an MPLS dataplane. To enable SRv6 network programming in an IPv6 domain, include the `srv6` statement at the `[edit protocols isis source-packet-routing]` hierarchy level. To advertise the Segment Routing Header (SRH) locator with a mapped flexible algorithm, include the `algorithm` statement at the `[edit protocols isis source-packet-routing srv6 locator]` hierarchy level.

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	To configure a TI-LFA backup path for SRv6 in an IS-IS network, include the `transit-srh-insert` statement at the `[edit protocols isis source-packet-routing srv6]` hierarchy level. [See How to Enable SRv6 Network Programming in IS-IS Networks.] • Support for SRv6 network programming and Layer 3 Services over SRv6 in BGP. You can configure BGP-based Layer 3 service over an SRv6 core. You can enable Layer 3 overlay services with BGP as the control plane and SRv6 as the data plane. SRv6 network programming provides flexibility to leverage segment routing without deploying MPLS. Such networks depend only on the IPv6 headers and header extensions for transmitting data. To configure IPv4 and IPv6 transport over an SRv6 core, include the `end-dt4-sid` *`sid`* and the `end-dt6-sid` *`sid`* statements at the `[edit protocols bgp source-packet-routing srv6 locator name]` hierarchy level. To configure IPv4 VPN and IPv6 VPN service over an SRv6 core, include the `end-dt4-sid` *`sid`* and the `end-dt6-sid` *`sid`* statements at the `[edit routing-instances` *`routing-instance-name`* `protocols bgp source-packet-routing srv6 locator` *`name`*`]` hierarchy level. [See Understanding SRv6 Network Programming and Layer 3 Services over SRv6 in BGP.] • OAM ping support for segment routing with IPv6 (SRv6) network programming. You can perform an Operations, Administration and Management (OAM) ping operation for any SRv6 segment identifier (SID) whose behavior allows upper layer header processing for an applicable OAM payload. As segment routing with IPv6 data plane (SRv6) adds only the new type-4 routing extension header, you can use the existing ICMPv6-based ping mechanisms for an SRv6 network to provide OAM support for SRv6. Ping with O-Flag (segment header) is not supported.

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	[See ITU-T Y.1731 Ethernet Service OAM Overview and How to Enable SRv6 Network Programming in IS-IS Networks.] • Support for SRv6 traceroute. We support the traceroute mechanism for segment routing for IPv6 (SRv6) segment identifiers. You can use traceroute for both UDP and ICMP probes. By default, traceroute uses UDP probes. For ICMP probes, use the `traceroute` command with the `probe-icmp` option. [See How to Enable SRv6 Network Programming in IS-IS Networks.] • SRv6 support for static SR-TE policy. You can configure static segment routing–traffic engineering (SR-TE) tunnels over an SRv6 data plane. Use the following configuration commands to enable SRv6 support: • For an SR-TE policy: `set protocols source-packet-routing srv6` • For an SR-TE tunnel: `set protocols source-packet-routing source-routing-path lsp` *`name`* `srv6` • For an SR-TE segment list: `set protocols source-packet-routing source-routing-path segment-list srv6` [See Understanding SR-TE Policy for SRv6 Tunnel.]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
Services applications	• Inline active flow monitoring support. [See Understand Inline Active Flow Monitoring.] • Juniper Resiliency Interface support. [See Juniper Resiliency Interface.] • Inline monitoring services support for packet mirroring with metadata. [See Inline Monitoring Services Configuration.] • Support for additional RPCs for the gNOI certificate management (`cert`) service. Junos OS Evolved supports the following gRPC Network Operations Interface (gNOI) `cert` service RPCs: • `CanGenerateCSR()` —Query if the target device can generate a certificate signing request (CSR) with the specified key type, key size, and certificate type. • `RevokeCertificates()`—Revoke certificates on the target device. [See gNOI Certificate Management (Cert) Service.] • CFM support: • Up maintenance association end points (MEPs) in distributed periodic packet management (PPM) • Distributed Y.1731 on synthetic loss measurement (SLM), delay measurement (DM), and loss measurement (LM) • Down MEPs on bridges, circuit cross-connect (CCC) , and Ethernet VPN (EVPN) • Distributed session support for connectivity fault management (CFM) on aggregated Ethernet • Enhanced CFM mode

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• IPv4 (`inet`) support for Data Model (DM) and synthetic loss message (SLM) • Action profile for marking a link down, except for EVPN and bridge up MEP • LM colorless mode • DM and LM on aggregated Ethernet if all active child links are on the same Packet Forwarding Engine • Supported CFM protocol data units (PDUs), as follows: • Continuity check messages (CCM) • LBM • LBR • Link Trace Message (LTM) • Link Trace Reply (LTR) • 1DM (one-way delay measurement) • Delay measurement message (DMM) • Delay measurement reply (DMR) • LMM • LMR • Synthetic loss message (SLM) • Synthetic loss reply (SLR) • Enterprise and service provider configurations • VLAN normalization • VLAN transparency for CFM PDUs

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• CoS forwarding class (FC) and CoS packet loss priority (PLP) for CFM • CFM session on child physical interface in distributed mode • SNMP • Chassis ID or Send ID type, length, and value • Trunk mode • Maintenance association intermediate point (MIP) [See Connectivity Fault Management (CFM).] • Support for enhanced CFM. The feature extends CFM support to inline mode. Support includes: • Up and down maintenance association end points (MEPs) on bridges, circuit cross-connect (CCC), and Ethernet VPN (EVPN) in inline mode • ITU-T Y.1731 on synthetic loss measurement (SLM) and delay measurement (DM) • Inline session support for connectivity fault management (CFM) on aggregated Ethernet • Enhanced CFM mode by default • Supported inline performance monitoring (PM) sessions, as follows: • PM Tx • PM Rx • PM responder • IPv4 (`inet`) and IPv6 (`inet6`) support for continuity check messages (CCM), delay measurement (DM), and synthetic loss message (SLM)

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• DM on aggregated Ethernet with at least one child link on the anchor Packet Forwarding Engine • Action profile for marking a link down, except for EVPN and bridge up MEP • Supported CFM protocol data units (PDUs) for inline handling, as follows: • CCM • Delay measurement message (DMM) • Delay measurement reply (DMR) • Synthetic loss message (SLM) • Synthetic loss reply (SLR) • Enterprise and service provider configurations • VLAN normalization • VLAN transparency for CFM PDUs • Combination of up MEP, down MEP, or maintenance association intermediate point (MIP) configuration over the same interface [See Connectivity Fault Management (CFM).]
Security services	• Support for DDoS IS-IS classification and higher DDoS bandwidth for Layer 2 and Layer 3 protocols. [See show ddos-protection protocols isis and protocols (DDoS) (ACX Series, PTX Series, and QFX Series).]
Software installation and upgrade	• Support for secure BIOS and secure boot implementation based on the UEFI 2.4 standard. [See Secure Boot.]

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
VPNs	• MPLS-based Layer 3 VPNs support includes: • MPLS over Layer 3 VLAN-tagged subinterfaces • Per-next-hop label allocation • Mapping of the label-switched interface (LSI) logical interface label to the VPN routing and forwarding (VRF) routing table using the `vrf-table-label` statement • ICMP tunneling and MPLS traceroute • Disabling time-to-live (TTL) decrementing using `no-propagate-ttl` [See Layer 3 VPNs Feature Guide for Routing Devices.] • Carriers-of-carriers and inter-AS VPN supported features include: • Carrier-of-carriers VPN service • Interprovider Layer 3 VPN Option A • Interprovider Layer 3 VPN Option B • Interprovider Layer 3 VPN Option C However, traffic statistic collection for BGP labeled unicast is not supported for carrier-of-carrier VPNs and interprovider traffic. [See Carrier-of-Carrier VPNs.] • Layer 2 VPN feature support includes: • Transport of Layer 2 frames over MPLS (LDP signaling) • Layer 2 VPNs over tunnels (BGP signaling) • Simple Ethernet and VLAN-based cross-connect (also known as connections)

Table 1: PTX10002-36QDD Feature Support *(Continued)*

Feature	Description
	• Local and remote switching • Ethernet and VLAN CCC • Single-tagged CCC logical interfaces • Control word • Regular and aggregated Ethernet interfaces • Layer 2 protocol pass-through • Layer 2 circuit backup interface and backup neighbor • Layer 2 circuit statistics and CoS • VCCV with type 2 and type 3 [See Layer 2 VPNs and VPLS User Guide for Routing Devices and TCC Overview.]

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

Chassis

- **Power redundancy and resiliency support (PTX10016)**—PTX10016 with JNP10K-PWR-AC3 power supply modules (PSMs) supports the following features:
  - N+1 power redundancy. You can enable either source redundancy or feed redundancy for the PSM.
  - Resiliency support for FRU components
  - PSM watchdog

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

- **Support for powering on, powering off, or restarting Packet Forwarding Engine (PTX10002-36QDD)**—You can power off, power on, or restart the Packet Forwarding Engines in the router by following these steps:

1. Configure the *pair* of Packet Forwarding Engines that you want to restart or power off/on—for example:
   - `set chassis fpc 0 pfe 0 power on`
   - `set chassis fpc 0 pfe 1 power on`

   NOTE: The four Packet Forwarding Engines are numbered 0–3. You configure them in pairs—0 and 1; 2 and 3.

2. Issue the power on, power off, or restart command—for example:
   - `request chassis fpc slot 0 pfe 0 power on`

3. Enter **yes** when the following question appears on the screen:
   - ```
     Warning: pfe 1 will also be offlined. Do you wish to continue?
             [yes,no]
     ```

   NOTE: You can also set the `reset-pfe` action to reset a PFE when a chassis error occurs—configure the `action` statement at `[edit chassis fpc` *`slot-number`* `error` *`error-severity-level`*`]` hierarchy level.

[See request chassis fpc and action (chassis error).]

Ethernet Switching and Bridging

- **Support for basic Layer 2 features (PTX10002-36QDD)**—The following Layer 2 basic learning, bridging and flooding features are supported:
  - Enterprise style bridging (support both trunk and access mode)
  - Service provider style bridging (also known as sub-interface mode)
  - Handle BUM (broadcast, unknown unicast and multicast) traffic, including split horizon
  - MAC learning and aging
  - Static MAC addresses
  - Trunk port and VLAN membership
  - 802.1Q Ethertype - 8100
  - 802.1Q VLAN tagging: Single tagging with normalized to bridge domain tag at ingress
     ```

- Clear all MAC address information
- Global MAC limit
- Global source MAC aging time
- MAC moves
- LACP and LLDP
- Disable MAC learning at global and interface level
- Native VLAN ID for Layer 2 logical interfaces
- Single VLAN-tagged Layer 2 logical interfaces
- Interface statistics

  > **NOTE**: The `show ethernet-switching statistics` command and child logical interface statistics for aggregated Ethernet are not supported.

- Flexible Ethernet services

  > **NOTE**: Enterprise-style Layer 2 logical interfaces cannot be allowed under `flexible-ethernet- services` encapsulation.

- Virtual switch
- Persistent MAC learning (sticky MAC)
- Service provider bridging:
  - Multiple logical interfaces on a same physical interface which are part of same bridge domain
  - Ethernet bridge encapsulation

[See Layer 2 Bridging, Address Learning, and Forwarding User Guide.]

- **Support for interface MAC limit action (PTX10002-36QDD)**—You can specify the action (drop, drop and log, log, or shut down) that Junos OS Evolved takes when packets with new source MAC addresses are received after the MAC address limit is reached.

  [See Configuring MAC Limiting and packet-action.]

- **Support for IRB (PTX10002-36QDD)**—Support for IRB enables routing of Layer 3 traffic between a bridge domain and another routed interface. Support includes:

- All Layer 2 protocols already supported on the router
- Layer 3 protocols: BGP, IGMP, IS-IS, OSPF, PIM, and RIP
- Per-IRB logical interface MAC and statistics
- IRB Layer 3 multicast support with flooding only
- Address family support for IPv4 and IPv6, and support for IPv4 MTUs and IPv6 MTUs with different MTU values
- IRB interface in VRF routing instances
- Directed subnet broadcast support with IRB
- Support for VRRP on IRB

[See Integrated Routing and Bridging, Configuring a Layer 2 Virtual Switch with a Layer 2 Trunk Port, and Understanding VRRP.]

- **Support for LLDP, xSTP, and BPDU protection (PTX10002-36QDD)**—Support includes:
  - RSTP, VSTP, MSTP, STP, root protection for STP, concurrent configuration of RSTP and VSTP, virtual switch, and BPDU protection for spanning-tree protocols
  - Bridge protocol data unit (BPDU) protection for EVPN-VXLAN
  - LLDP support, including:
    - LLDP on em0 interfaces
    - Disabling of LLDP time, length, and value (TLV) messages

  [See Configuring STP, Understanding BPDU Protection for EVPN-VXLAN, and Device Discovery Using LLDP.]

Interfaces

- **Support for media access control (MAC) accounting for source and destination MAC addresses for Layer 3 interfaces (PTX100021-36QDD)**—We support media access control (MAC) accounting for source and destination MAC addresses for Layer 3 interfaces and aggregated Ethernet interfaces. To enable MAC accounting, use the `mac-learn-enable` configuration statement under the `[edit interfaces` *`interface-name`* `gigether-options ethernet-switch-profile]` or the `[edit interfaces aex aggregated-ether-options ethernet-switch-profile]` hierarchy level.

  [See show interfaces mac-database.]

Layer 2 VPN

- **VLAN ID lists for Layer 2 Circuits (PTX10002-36QDD)**- Starting in Junos OS Evolved 24.2R2, we support VLAN ID lists for Layer 2 Circuits. VLAN ID lists allow you to link multiple VLAN ID's to a single logical interface for Layer 2 traffic.

  [See vlan-id-list (Ethernet VLAN Circuit), vlan-id-list, and Configuring VLAN Identifiers for VLANs and VPLS Routing Instances.]

MACsec

- **MACsec bounded delay protection (PTX10002-36QDD)**—You can enable Media Access Control Security (MACsec) bounded delay protection to protect your network against man-in-the-middle attacks. When you enable MACsec bounded delay protection, the device guarantees that a frame will not be delivered after a delay of two seconds or more. MACsec periodically compares the number of frames transmitted to the number received. If a frame is sent but not received within two seconds, such as during a man-in-the-middle-attack, MACsec drops the packet.

  [See Configuring Bounded Delay Protection.]

MPLS

- **Supports next-hop-based dynamic tunnels with IPv6 in the underlay network (PTX10002-36QDD)**—You can encapsulate IPv4 and IPv6 packets inside the IPv6 packets between two IPv6 nodes. This encapsulation mechanism helps to create next-hop-based dynamic tunnels with IPv6 in the underlay network.

  [See Next-Hop-Based Dynamic Tunnels and show dynamic-tunnels database.]

Multicast

- **Multicast support for Next-Generation MVPN (NGMVPN) (PTX10002-36QDD)**— Support includes:
  - IR, RSVP-P2MP, and LDP-P2MP provider tunnel
  - Inclusive and selective PMSI tunnel
  - Rendezvous-point tree (RPT)-shortest-path tree (SPT) mode
  - Restart individual PFE instances
  - Turnaround provider edge (PE) device
  - RP mechanisms, including auto rendezvous point (RP), bootstrap router (BSR), and embedded RP

  [SeeMultiprotocol BGP MVPNs Overview, Understanding Next-Generation MVPN Concepts, andUnderstanding Next-Generation MVPN Control Plane.]

Network Management and Monitoring

- **Support for additional family in port mirroring (PTX10002-36QDD)**—You can configure family `any` (as well as the earlier family options, `inet` and `inet6`) for local port mirroring and remote port mirroring. You use family `any` for family `any`, `ccc`, `ethernet-switching`, or `mpls`.

  > **NOTE**: You use the family any configuration option to process all 4 families.

  You no longer configure port mirroring by using the `[edit forwarding-options port-mirroring analyzer]` hierarchy on the PTX devices.You now use `[edit forwarding-options port-mirroring]` for local port mirroring or `[edit forwarding-options port-mirroring instance *instance-name*]` for remote port mirroring, with both of those configurations also requiring a firewall filter.

  The following configuration statements are no longer part of the port-mirroring configuration on PTX:

  - `next-hop` for family `any`
  - `family vpls`
  - `no-filter-check`
  - `hosted-service`
  - `server-profile`

  [See Example: Configure Port Mirroring with Family any and a Firewall Filter and port-mirroring.]

Precision Time Protocol (PTP)

- **Support for G.8275.1 profile, PTP over Ethernet encapsulation, and hybrid mode over LAG with PTP over Ethernet (PTX10002-36QDD)**—Starting in Junos OS Evolved Release 24.2R2, these features are added to the router.

  [See G.8275.1 Telecom Profile, Guidelines for Configuring PTP over Ethernet, and Hybrid Mode.]

Routing Policy and Firewall Filters

- **Layer 2 and Layer 3 support for flood policers (PTX10002-36QDD)**—You can configure firewall filters for flood policers on Layer 2 (family `ccc`) and Layer 3 (family `any`) traffic, in both the ingress and egress directions. Most match conditions (except `packet-length`) and most actions are supported.
- **Firewall filtering using flood policer, IRB, and service provider egress filtering (PTX10002-36QDD)**—You can use the flood policer feature to control flooding of the network with broadcast, unknown unicast, and multicast (BUM) traffic, and this control includes the EVPN flood policer. We now support inner VLAN ID and inner VLAN priority on ingress and egress and service provider style

egress filters. Service provider style egress filters are Layer 2 filters attached in the egress direction for L2 interfaces configured in the service provider style. IRB filters are attached to an IRB interface configured for transitioning packets from Layer 2 to Layer 3 forwarding and vice versa (both entering or exiting the L3 interface) to control flooding of traffic in a given bridge domain. You can attach filters to IRB interfaces for both ingress and egress, but the execution of filters is different for each direction.

NOTE: EVPN-MPLS configurations also support flood policers.

[See **Policer Support for Aggregated Ethernet Interfaces Overview**.]

- **Match the flow-label field in an IPv6 packet (PTX10002-36QDD, PTX10008)**—Support is added for matching the 20-bit flow-label field in the header of an IPv6 packet. Two new match conditions have been added - `flow-label` *`flow label value`* and `flow-label` *`flow label value`* `mask` *`mask value`*.

  [See Firewall Filter Match Conditions for IPv6 Traffic.]

- **Increase firewall filter scale over performance (PTX10002-36QDD)**—You can use `scale-mode` to accommodate more firewall filter terms, when the need is to provide more scale than performance. You can use `no-incremental-update` to prevent the filter from undergoing incremental update.

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

- **Support added to hierarchical policers for applying user-selectable bandwidth for premium and non-premium traffic (PTX10002-36QDD)**—You can use the new firewall filter action `policer-charge` to subtract available bandwidth credits and make it available to the aggregate policer.

  [See policer-charge.]

Services Applications

- **Inline active flow monitoring IPFIX and version 9 template support forCoS policy-map name reporting in the ingress direction (PTX10002-36QDD)**—We support a new Juniper-specific enterprise Information Element ID, 32765, in the data record templates `ip4-template` and `ipv6-template`. This new IE ID is 4 bytes long and contains the first 4 characters of the policy-map name. Therefore, the first 4 letters of your policy-map names should be unique. You configure this new IE ID with the `include-policy-map-name` statement at the `[edit services flow-monitoring (version-ipfix|version9)` *`template-name`* `data-record-fields]` hierarchy level. You configure policy maps at the `[edit class-of-service policy-map]` hierarchy level.

  [See data-record-fields, Understand Inline Active Flow Monitoring, and Assigning Rewrite Rules on a Per-Customer Basis Using Policy Maps.]

Software Installation and Upgrade

- **Zero touch provisioning on WAN interfaces (PTX10002-36QDD)**—Zero Touch Provisioning (ZTP) dynamically detects the port speed of WAN interfaces and uses this information to create ZTP client ports with the same speed. ZTP automatically cycles through the WAN ports until it receives Dynamic Host Control Protocol (DHCP) options from the DHCP server. The device uses the DHCP options to perform the bootstrap process.

  [See **Zero Touch Provisioning**.]

- **Secure Zero Touch Provisioning (PTX10002-36QDD)**—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 zero touch provisioning.

  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 on the network device. Juniper Networks issues a digital voucher to customers for each eligible network device.

  See Secure Zero Touch Provisioning and Generate Secure ZTP Vouchers.

- **Switching between Secure ZTP and ZTP on secure platforms (PTX10002-36QDD)**—You can switch between using secure zero touch provisioning (SZTP) and zero touch provisioning (ZTP) on secure platforms. To override the default behavior of your secure device, you can issue the `request system zeroize ztp-option secure disable` command. When you issue this command, the CLI checks to see if the default platform behavior is secure. If the default platform is secure, the device will run ZTP after you reboot. If the default platform is not secure, the process ends. When you issue the `request system zeroize ztp-option secure enable` command, the CLI checks to see if the platform behavior is secure. If the default platform is secure, the process ends. If the platform isn't secure, you will receive an error that says the platform is not secure and cannot switch to SZTP. The process ends.

  See Switching between Secure Zero Touch Provisioning and Zero Touch Provisioning

Additional Features

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

- **EVPN Proxy ARP and Proxy NDP (PTX10002-36QDD)**

  [See EVPN Proxy ARP and ARP Suppression, and Proxy NDP and NDP Suppression.]

- **EVPN-VXLAN L2 gateways and L3 gateways with EVPN Type 5 routes (PTX10002-36QDD).**

  Support includes:

  - Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) Layer 2 and Layer 3 gateway operations in edge-routed bridging (ERB) and centrally routed bridging (CRB) fabrics

- EVPN instances using the MAC-VRF instance type with VLAN-based, VLAN-bundle, or VLAN-aware bundle service types
- Pure EVPN Type 5 (IP prefix) route virtual routing and forwarding (VRF) model
- Integrated routing and bridging (IRB) for IPv4 and IPv6 data traffic
- Q-in-Q dual tagging for VXLAN network identifier (VNI) mapping with service provider style logical interface configurations only
- Overlapping VLAN IDs across MAC-VRF instances
- Underlay reachability over ECMP
- Active/active multihoming with Ethernet segment identifiers (ESIs) per physical interface
- Proxy Address Resolution Protocol (ARP) and proxy Network Discovery Protocol (NDP), and ARP or NDP suppression
- Multicast IRB support without IGMP snooping or MLD snooping
- IEEE 802.1p and Differentiated Services code point (DSCP) class of service (CoS) on EVPN-VXLAN tunnel interfaces, with both service provider style or enterprise style interface configurations (including classification and rewrite operations, but not DSCP copy support)

[See EVPN User Guide.]

- **Overlays: Static-VXLAN Layer2 Gateway** (PTX10002-36QDD)

  [See Static VXLAN, remote-vtep-list, and static-remote-vtep-list.]

- **EVPN Proxy ARP and Proxy NDP** (PTX10002-36QDD)

  [See EVPN Proxy ARP and ARP Suppression, and Proxy NDP and NDP Suppresion .]

- **Support for EVPN-VPWS**(PTX10002-36QDD)

  [See Overview of VPWS with EVPN Signaling Mechanisms.]

- **Support for VPLS** (PTX10002-36QDD,)—You can configure VPLS on the PTX10002-36QDD.
  - To configure VPLS, configure the `instance-type virtual-switch` statement at the `[edit routing-instances` *`routing-instance-name`*`]` hierarchy level.
  - In this release, we support single bridge domains. You must configure `service-type single` statement at the `[edit routing-instances` *`routing-instance-name`* `vpls]` hierarchy level.
  - When you configure VPLS support on the PTX 10000 series, you must enable `control-word` at the `[edit routing-instances` *`routing-instance-name`* `protocols vpls]` hierarchy level.

- Encapsulation of `ethernet-vpls` and `vlan-vpls` is not supported on CE interfaces.
- To display VPLS MAC address information, use the `show ethernet-switching table` command.

[See Introduction to Configuring VPLS

- **Support for flexible firewall filter match conditions**(PTX10002-36QDD)

  [See Flexible Firewall Filter Match Conditions.]

- **Support for fast-lookup-filter on Any, ethernet switching, and CCC firewall family filters** (PTX10002-36QDD)

  [See fast-lookup-filter.]

- **Support for VNI based match for EVPN-VXLAN** (PTX10002-36QDD)

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

- **Support for Q-in-Q tunneling (PTX10002-36QDD) .**

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

- **Support for tunnel decapsulation using firewall filters for GRE and UDP tunnels** (PTX10002-36QDD)

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

- **Support for output filter-based GRE** (PTX10002-36QDD)—For an outgoing packet matching the filter term, the packet is encapsulated inside an IP + GRE header as specified by the tunnel configuration. IP lookup is performed on the outer header and packet is forwarded accordingly. The IP lookup for GRE-encap capable route is limited to the implicit default routing-instance.

  [See Understanding Filter-Based Tunneling Across IPv4 Networks.]

- **Support for configuring output filter action with non-default routing instance or a specified routing instance (PTX10002-36QDD)**

  [See Firewall Filter Terminating Actions.]

- **Support for filter-based forwarding (PTX10002-36QDD, PTX10004, PTX10008, and PTX10016)**

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

- **Firewall filter support for bitwise logical operations for TCP Flag match (PTX10002-36QDD, PTX10004, PTX10008, and PTX10016)**

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

What's Changed

IN THIS SECTION

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

Class of Service (CoS)

- Previously, the Junos OS Evolved system default scheduler was named "default" (no brackets), while the Junos OS system default scheduler is named "default" (with brackets). Now, the Junos OS Evolved system default scheduler is also named "default" (with brackets).

EVPN

- **EVPN system log messages for CCC interface up and down events**—Devices will now log EVPN and EVPN-VPWS interface up and down event messages for interfaces configured with circuit cross-connect (CCC) encapsulation types. You can look for error messages with message types EVPN_INTF_CCC_DOWN and EVPN_INTF_CCC_UP in the device system log file `/var/log/syslog`).

General Routing

- **Change to the commit process**—In prior Junos OS and 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.

- On Junos OS Evolved, password authentication for SCP based configuration archival is supported.

- **DDoS protection protocols statistics update (PTX Series)**—Starting in Junos OS Evolved Release 23.2R2, the `show ddos-protection protocols statistics` displays the `Max arrival rate` and `Arrival rate` output values as expected. Earlier to this release, the `Max arrival rate` and `Arrival rate` output values were displayed larger than expected.

  [See show ddos-protection protocols parameters.]

- In a firewall filter configured with a port-mirror-instance or port-mirror action, if l2-mirror action is also configured, then port-mirroring instance family should be any. In the absence of the l2-mirror action, port-mirroring instance family should be the firewall filter family.

- Configuring export profile parameters for dial-out telemetry traffic, such as 'dscp', 'forwarding-class', and 'payload-size', will now result in an error. Previously, these parameters were ignored because the telemetry traffic adhered to global configuration settings for host-bound traffic. This ensures clarity and prevents misconfiguration, aligning export profiles strictly with supported parameters.

- **Control Board offline delay for system stability (PTX10008)**—After initiating a node halt, you must wait 1 minute before doing Control Board (CB) offline. Attempting to offline the CB within this period will result in an error message. This delay helps maintain the stability and proper functioning of the system.

  [See request chassis cb.]

Routing Protocols

- **Update to IGMP snooping membership command options**—The `instance` option is now visible when issuing the `show igmp snooping membership ?` command. Earlier, the `instance` option was available but not visible when `?` was issued to view all possible completions for the `show igmp snooping membership` command.

  [See show igmp snooping membership.]

- **MLD snooping proxy and l2-querier source-address (ACX7024, ACX7100-32C, PTX10001-36MR, QFX5120-32C, and QFX5130-32CD)**—The `source-address` configured for `proxy` and `l2-querier` under the `mld-snooping` hierarchy should be an IPv6 link-local address in the range of fe80::/64. The CLI help text has been updated to "Source IPv6 link local address to use for proxy/L2 querier". In earlier releases, the CLI help text read, "Source IP address to use for proxy/L2 querier."

  [See source-address.]

User Interface and Configuration

- **Access privileges for request support information command (ACX Series, PTX Series, QFX Series)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance`, `view`, and `view-configuration` can execute request support information command.

Known Limitations

There are no known limitations in hardware or software 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.

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

- On all EVO platforms, port LED goes unlit/off instead of amber/on when port is disabled. PR1690655
- On all Junos OS Evolved platforms, snmp mib walk jnxOperatingState on Fan Tray X returns running(2), although fan tray X speed is set to full-speed. It is expected runningAtFullSpeed(5) when fan tray speed is set to full-speed.PR1701983
- DNS resolution over a routing-instance fails.PR1733616
- When DHCP trace options are enabled, the jdhcpd might create a core file. In general, traceoptions must be enabled for debugging only. They should be disabled once debugging is complete.PR1771121
- On Junos OS Evolved PTX Series platform, the BGP session flap can be seen when inline Bidirectional Forwarding Detection (BFD) is configured under routing instance without loopback interface (lo0) leading to partial traffic drop. The issue is seen only when the interface is within the routing-instance.PR1811245
- On Junos Evolved PTX10003 platform the command `indirect-next-hop-change-acknowledgements` is required in the Junos default configuration. If the command is missing, it will result in packet loss.PR1836337
- On PTX10004, PTX10008, and PTX100016 platforms with LC1202 line card, retimer/gearbox ports on LC1202 line card take longer duration (approximately 1500 msec) to bring an interface back up after short LOS insertion from peer device. This breaks sub-second hold-time down feature. The

code fix enabled 'fast linkup' feature of retimer/gearbox ports. It helped the link to come up faster. Ideally retimer/gearbox ports take 1.5 sec to come up, but with this feature, links come up in 1 sec. PR1846379

Network Management and Monitoring

- Error message "CMDOUT (error: error renaming temp state file /var/lib/logrotate.status.tmp)" is generated every 15 minutes.PR1747722
- On Junos OS Evolved platforms, SNMP cold start trap is observed on console log upon system reboot, but it is not sent out to external server.PR1788308

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)

- One CoS drop-profile might not work on PTX EVO platforms. PR1814641

Flow-based and Packet-based Processing

- A router running sampling may see the msvcs-db daemon run at 99.9 percentage for an extended period PR1816542
- The flow record outputs are not displayed correctly on Junos OS Evolved platforms. PR1828032

General Routing

- Few frequencies might fail to meet the mask. PR1624478
- Telemetry data is not exported in an IS-IS scaled segment routing scenario. PR1745615
- [Junos OS Evolved] PTX10004/8/16 - Minor alarm LED on front panel module (FPM) is glowing yellow, although there is no active alarms/errors on the system. PR1782498
- Higher AE traffic convergence observed in ALB configured AE interface. PR1784498
- Channelized interface 4x10G remains DOWN with good signal levels. PR1794352
- Bootup time increases by 13 percent when filesystem encryption is enabled. PR1796086
- Legacy inet6 address seen under vmb0 while modifying mgmt-0 IPv6 address with dadfailed. PR1796934
- Filesystem encryption is getting enabled again when filesystem encryption is enabled and the primary is being restored from a snapshot. PR1797258
- On Junos OS Evolved PTX1003-160C and PTX10003-80C platforms FPC instability lead to CPU reset and service interruption. PR1797283
- During PSM health check chassis power consumption may spike at 25 percent to 30 percent according to the CLI output. PR1798298
- On certain Junos OS Evolved ACX Series and PTX Series platforms USB installation does not work on encrypted disk. PR1798539
- USB media installation shows up minor alarm "Host 0 Voltage Threshold Crossed". PR1799443
- DHCP client on mgmt0 interface fails to start and dhcp-managerd generates a core file. PR1799681
- PTX EVO DDoS stats values of "Arrival rate" and "Max arrival rate" on system-wide and FPC showing larger values than expected. PR1801290
- The optics temperature sensor name renamed from 'et-x/y/z' to 'xcvr-x/y/z'. PR1802195

- Time-zone info changes to default UTC after upgrade is done with restart-upgrade. PR1803511
- The sysapp-mib.re core file is generated for EVO devices. PR1808788
- The syslog "LICENSE_EXPIRED" are not seen when license gets expired". PR1808956
- Interface going down after PTP deactivates and re-activates with G.8275.1 profile. PR1809309
- Interfaces take a long time to come up after reboot when configured in scaled IFL environment. PR1809423
- On PTX10001 EVO platform, traffic might drop unexpectedly due to uRPF failure. PR1809955
- Shared policer bandwidth doesn't work after removing an interface from aggregated Ethernet. PR1812144
- ZR optics doesn't work when wavelength 1548.91 is configured. PR1812634
- Traffic drops in the MVPN path due to the interface flap leading to composite next-hop changes. PR1814222
- The evo-cda-bt process crash and error logs are observed with AE member interfaces on non-zero Packet Forwarding Engines. PR1815166
- VRRP is not working for VRRP group 0 when specific Junos OS Evolved platforms are working as master. PR1816310
- Proxy-arp restricted is not working as expected. PR1817691
- Unit test failure found for component "app-controller-test". PR1818196
- The picd process crash will be seen on PTX10001-36MR. PR1818352
- Negative values are seen for jnxOperatingUpTime SNMP mib after ~248 days uptime. PR1819254
- 2x100G SFP port 0/1/9 channel 0 will go down on the Junos OS Evolved PTX10001-36MR platform. PR1819780
- The aftman process crashes when IPv6 (IPv6 address with prefix length is greater than or equal to 88) filter configuration on the dsc interface. PR1820118
- Multicast routes can be out of sync due to the quick aggregate Ethernet interface flap. PR1820376
- Per-Segment-list telemetry for colored tunnel doesn't work. PR1820791
- BFD protocol sessions flap continuously when operating in hardware-assisted inline mode. PR1822526
- PTX10001-36MR-K major alarm Host 0 Ethernet Interface Link Down. PR1822938

- The "request system debug-info" takes too long time than expected. PR1824540
- NETCONF output for unsuccessful ping is empty. PR1827914
- PTX Series devices acting as transit nodes display incorrect MPLS traceroute or TTL. PR1829924
- On PTX Series platform running Junos OS EVO OAM LFM event PDU may be generated with wrong values. PR1830990
- SNMPWALK LED not matching physical LED status with d2d failure. PR1831436
- Possibility of a rare crash in one of the firewall related apps. PR1832801
- snmp mib walk on jnxDomCurrentLaneRxLaserPower any OID under XcvrDiagLaneData does not show object instance values for all lanes except lane 0. PR1835757
- BUM traffic to remote leaf vtep in an EVPN-vxlan fabric is dropped on all PTX Series Evolved platforms. PR1836051
- CFM session fails to install after changing the child links of the aggregated Ethernet bundle. PR1836692
- Transport MACSEC packet drops in MAC-VRF instance with trapcode dlu.ucode.not_routable. PR1836809
- The rpdagent process is getting restarted after switchover. PR1836997
- "bt_mtip_chpcs_hw_clear_stats: failed" error will be seen post rebooting the device. PR1838394
- Traffic issue is seen when P2MP transit LSP with aggregated Ethernet as one of the branch on certain Junos OS Evolved PTX platforms. PR1840095
- Multihop BFD remains down when it's associated with a static route in the routing instance. PR1840295
- The evo-aftmand-bt/evo-aftmand-bx crash observed with SCU/DCU feature on IPv6 prefixes. PR1841145
- Error logs seen with Port-mirror. PR1841713
- Core files generated are incomplete after unzip. PR1843642
- On rare occasions under load conditions after a switchover, the ehmd process on the standby Routing Engine may crash. PR1843884
- The cfmman memory leaks when CFM remote-mep is configured and adjacency goes down. PR1846960

- Traffic going over LDP or LDPoRSVP route matching the CBF is getting impacted when PTX EVO platform working as PHP router with CBF configuration. PR1847169
- Traffic loss observed over load-balanced ESI LAG towards Provide Edge router in an EVPN-MPLS path on Junos OS Evolved PTX Series platforms PR1849188
- Post configuration changes on an AE interface MPLS traffic is discarded for other interfaces/AE interface on a different FPC PR1856732

Infrastructure

- Junos OS Evolved: TCP session state is not always cleared on the Routing Engine leading to DoS (CVE-2024-47502). PR1785913
- fibd crash is seen after excessive logging in scaled scenarios. PR1814970

Interfaces and Chassis

- On PTX10003 4x10GE/4x25GE interface drop the traffic in working lanes when new lane is configured with 400GE as neighbor interface. PR1810718

Network Management and Monitoring

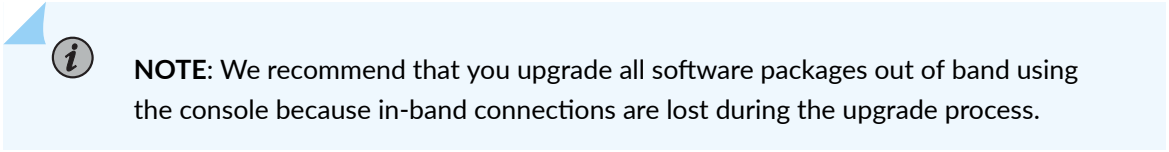
- PTX10004 - Host-name is not updated in picd logs. PR1815238
- The mib2d crash is observed on Junos OS Evolved platforms with duplicate SNMP request. PR1815524
- Netconf over ssh stop working with "sshd[(pid)]: fatal: /etc/ssh/netconf_config line 10: Directive 'Ciphers' is not allowed within a Match block" error. PR1831167
- The mib2d memory increase observed during 24 hours testing. PR1836012

Upgrade Your Junos OS Evolved Software

Products impacted: ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348, ACX7509, PTX10001-36MR, PTX10003, PTX10004, PTX10008, PTX10016, and PTX10002-36QDD.

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.

- 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

26 May 2025—Revision 4, Junos OS Evolved Release 24.2R2

26 April 2025—Revision 3, Junos OS Evolved Release 24.2R2

17 April 2025—Revision 2, Junos OS Evolved Release 24.2R2

28 February 2025—Revision 1, Junos OS Evolved Release 24.2R2